Exhibit 91:

Contract for MSOR database
[MSP 355-455]

STATE OF MICHIGAN PROCUREMENT

Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913

P.O. BOX 30026 LANSING, MICHIGAN 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. 190000001014

between

THE STATE OF MICHIGAN

and

CONTRACTOR	
	LexisNexis Coplogic Solutions Inc.
	1000 Alderman Drive
	Alpharetta, GA 30005
	Bob Holtgrave
	502-608-2624
	robert.holtgrave@lexisnexisrisk.com
	VS0091805

STATE			
	Program Manager	F/Lt. Alan Renz	MSP
		517-648-5871	
		Renza1@michigan.gov	
	Contract Administrator	Sean Regan	DTMB
		517-243-8459	
		regans@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: Sexual Offender Registry System			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
11/18/2019	11/17/2024	2, 1 Year	
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45			
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-card ☐ Payment Request (PRC) ☐ Other			☐ Yes ☒ No
MINIMUM DELIVERY REQUIREMENTS			
MISCELLANEOUS INFORMATION			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			**$1,900,000.00**

Does v Whitmer
Case No. 22-cv-10209

MS
D

Approved DOC 10-24-19

FOR THE CONTRACTOR:

LexisNexis Coplogic Solutions Inc.
Company Name

Authorized Agent Signature

William S. Madison, EVP
Authorized Agent (Print or Type)

10/21/2019
Date

FOR THE STATE:

Signature

Simon Baldwin, Category Manager, IT
Name & Title

DTMB Central Procurement
Agency

11/1/2019
Date

STATE OF MICHIGAN

Table of Contents for Contract No. 190000001014

STATE OF MICHIGAN

Contract Terms
COTS Software Contract

This Software Contract (this "**Contract**") is agreed to between the State of Michigan (the "**State**") and Lexis Nexis Coplogic Solutions ("**Contractor**"). This Contract is effective on November 18, 2019 ("**Effective Date**"), and unless earlier terminated, will expire on November 17, 2024 (the "**Term**").

This Contract may be renewed for up to 2 additional, 1-year periods. Renewal must be by written notice from the State and will automatically extend the Term of this Contract.

1. Definitions. For the purposes of this Contract, the following terms have the following meanings:

"**Acceptance**" has the meaning set forth in **Section 12.5**.

"**Acceptance Tests**" means such tests as may be conducted in accordance with **Section 12** and the Statement of Work to determine whether the Software meets the requirements of this Contract and the Documentation.

"**Affiliate**" of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For purposes of this definition, the term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect ownership of more than fifty percent (50%) of the voting securities of a Person.

"**Allegedly Infringing Materials**" has the meaning set forth in **Section 26.3(b)(ii)**.

"**API**" means all Application Programming Interfaces and associated API Documentation developed by Contractor exclusively for the State under this Contract, and as updated from time to time, to allow the Software to integrate with various State and Third-Party Software.

"**Approved Open-Source Components**" means Open-Source Components that may be included in or used in connection with the Software and are specifically identified in an exhibit to the Statement of Work and approved by the State.

"**Authorized Users**" means all Persons authorized by the State to access and use the Software under this Contract, subject to the maximum number of users specified in the applicable Statement of Work.

"**Business Day**" means a day other than a Saturday, Sunday, government recognized holiday or other day on which the State is authorized or required by Law to be closed for business.

"Business Owner" is the individual appointed by the agency buyer to (a) act as the agency's representative in all matters relating to the Contract, and (b) co-sign off on notice of Acceptance for the Software. The Business Owner will be identified in the Statement of Work.

"**Business Requirements Specification**" means the initial specification setting forth the State's business requirements regarding the features and functionality of the Software, as set forth in the Statement of Work.

"Change" has the meaning set forth in **Section 2.2.**

"Change Notice" has the meaning set forth in **Section 2.2(b).**

"Change Proposal" has the meaning set forth in **Section 2.2(a).**

"Change Request" has the meaning set forth in **Section 2.2.**

"Confidential Information" has the meaning set forth in **Section 20.1.**

"**Configuration**" means State-specific changes made to the Software without Source Code or structural data model changes occurring.

"**Contract**" has the meaning set forth in the preamble.

"**Contract Administrator**" is the individual appointed by each party to (a) administer the terms of this Contract, and (b) approve any Change Notices under this Contract. Each party's Contract Administrator will be identified in the Statement of Work.

"**Contractor**" has the meaning set forth in the preamble.

"**Contractor's Bid Response**" means the Contractor's proposal submitted in response to the Direct Solicitation.

"**Contractor Personnel**" means all employees of Contractor or any Permitted Subcontractors involved in the performance of Services hereunder.

"**Contractor's Test Package**" has the meaning set forth in **Section 11.2**.

"**Criminal Justice Information Data**" or "**CJI Data**" means data necessary for criminal justice agencies to perform their mission and enforce the laws.

"**Deliverables**" means the Software, and all other documents and other materials that Contractor is required to or otherwise does provide to the State under this Contract and otherwise in connection with any Services, including all items specifically identified as Deliverables in the Statement of Work.

"**Dispute Resolution Procedure**" has the meaning set forth in **Section 31.1**.

"**Documentation**" means all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

"**DTMB**" means the Michigan Department of Technology, Management and Budget.

"**Effective Date**" has the meaning set forth in the preamble.

"**Fees**" means collectively, the License Fees, Implementation Fees, and Support Services Fees.

"**Financial Audit Period**" has the meaning set forth in **Section 29.1**.

"**Force Majeure**" has the meaning set forth in **Section 32.1.**

"**Harmful Code**" means any: (a) virus, trojan horse, worm, backdoor or other software or hardware devices the effect of which is to permit unauthorized access to, or to disable, erase, or otherwise harm, any computer, systems or software; or (b) time bomb, drop dead device, or other software or hardware device designed to disable a computer program automatically with the passage of time or under the positive control of any Person, or otherwise prevent, restrict or impede the State's or any Authorized User's use of such software.

"**HIPAA**" has the meaning set forth in **Section 19.1**.

"**Implementation Fees**" has the meaning set forth in **Section 16.2**.

"**Implementation Plan**" means the schedule included in the Statement of Work setting forth the sequence of events for the performance of Services under the Statement of Work, including the Milestones and Milestone Dates.

"Integration Testing" has the meaning set forth in **Section 12.1(c)**.

"**Intellectual Property Rights**" means all or any of the following: (a) patents, patent disclosures, and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, and domain names, together with all of the associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works and rights in data and databases; (d) trade secrets, know-how and other confidential information; and (e) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection provided by applicable Law in any jurisdiction throughout the world.

"**Key Personnel**" means any Contractor Personnel identified as key personnel in the Statement of Work.

"**Law**" means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree or other requirement or rule of any federal, state, local or foreign government or political subdivision thereof, or any arbitrator, court or tribunal of competent jurisdiction.

"**License Agreement**" has the meaning set forth in **Section 3.**

"**License Fee**" has the meaning set forth in **Section 16.1**.

"**Loss or Losses**" means all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

"**Maintenance and Support Schedule**" means, if applicable, the schedule attached as **Schedule B**, setting forth the Support Services Contractor will provide to the State, and the parties' additional rights and obligations with respect thereto.

"**Maintenance Release**" means any update, upgrade, release or other adaptation or modification of the Software, including any updated Documentation, that Contractor may generally provide to its licensees from time to time during the Term, which may contain, among other things, error corrections, enhancements, improvements or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

"**Milestone**" means an event or task described in the Implementation Plan under the Statement of Work that must be completed by the corresponding Milestone Date.

"**Milestone Date**" means the date by which a particular Milestone must be completed as set forth in the Implementation Plan under the Statement of Work.

"**New Version**" means any new version of the Software that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

"**Nonconformity**" or **"Nonconformities"** means any failure or failures of the Software to conform to the requirements of this Contract, including any applicable Documentation.

"**Open-Source Components**" means any software component that is subject to any open-source copyright license agreement, including any GNU General Public License or GNU Library or Lesser Public License, or other obligation, restriction or license agreement that substantially conforms to the Open Source Definition as prescribed by the Open Source Initiative or otherwise may require disclosure or licensing to any third party of any source code with which such software component is used or compiled.

"**Open-Source License**" has the meaning set forth in **Section 4.**

"**Operating Environment**" means, collectively, the platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in the Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software and system architecture and configuration.

"**Permitted Subcontractor**" has the meaning set forth in **Section 9.4**.

"**Person**" means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or other entity.

"**Pre-existing Intellectual Property**" means all original software, source code, logic, methods, procedures, and any other data and documents, in whatever form or format, related thereto, owned by Contractor before the Effective Date, the Core Framework, and anything created by Contractor outside the scope of this Contract.

"**Pricing**" means any and all fees, rates and prices payable under this Contract, including pursuant to any Schedule or Exhibit hereto.

"**Pricing Schedule**" means the schedule attached as **Schedule D**, setting forth the License Fees, Implementation Fees, Support Services Fees, and any other fees, rates and prices payable under this Contract.

"**Project Manager**" is the individual appointed by each party to (a) monitor and coordinate the day-to-day activities of this Contract, and (b) for the State, to co-sign off on its notice of Acceptance for the Software. Each party's Project Manager will be identified in the Statement of Work.

"**Representatives**" means a party's employees, officers, directors, partners, shareholders, agents, attorneys, successors and permitted assigns.

"**RFP**" means the State's request for proposal designed to solicit responses for Services under this Contract.

"**Services**" means any of the services Contractor is required to or otherwise does provide under this Contract, the Statement of Work, the Maintenance and Support Schedule (if applicable), or the Service Level Agreement (if applicable).

"**Service Level Agreement**" means, if applicable, the service level agreement attached as **Schedule E** to this Contract, setting forth Contractor's obligations with respect to the hosting, management and operation of the Software.

"**Site**" means the physical location designated by the State in, or in accordance with, this Contract or the Statement of Work for delivery and installation of the Software.

"**Software**" means Contractor's software set forth in the Statement of Work, and any Maintenance Releases or New Versions provided to the State and any Configurations made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract and the License Agreement. Software includes Contractor's Core Framework.

"**Source Code**" means the human readable source code of the Software to which it relates, in the programming language in which the Software was written, together with all related flow charts and technical documentation, including a description of the procedure for generating object code, all of a level sufficient to enable a programmer reasonably fluent in such programming language to understand, build, operate, support, maintain and develop modifications, upgrades, updates, adaptations, enhancements, new versions and other derivative works and improvements of, and to develop computer programs compatible with, the Software.

"**Specifications**" means, for the Software, the specifications collectively set forth in the Business Requirements Specification, Technical Specification, Documentation, Direct Solicitation or Contractor's Bid Response, if any, for such Software, or elsewhere in the Statement of Work.

"**State**" means the State of Michigan.

"**State Data**" has the meaning set forth in **Section 19.1**.

"**State Materials**" means all materials and information, including documents, data, know-how, ideas, methodologies, specifications, software, content and technology, in any form or media, directly or

indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

"**State Resources**" has the meaning set forth in **Section 10.1(a)**.

"**Statement of Work**" means any statement of work entered into by the parties and attached as a schedule to this Contract. The initial Statement of Work is attached as **Schedule A**, and subsequent Statements of Work shall be sequentially identified and attached as Schedules A-1, A-2, A-3, etc.

"**Stop Work Order**" has the meaning set forth in **Section 24**.

"**Support Services**" means the software maintenance and support services Contractor is required to or otherwise does provide to the State under the Maintenance and Support Schedule (if applicable) or the Service Level Agreement (if applicable).

"**Support Services Commencement Date**" means, with respect to the Software, the date on which the Warranty Period for the Software expires, or such other date as may be set forth in the Statement of Work.

"**Support Services Fees**" has the meaning set forth in **Section 16.3**.

"**Technical Specification**" means, with respect to any Software, the document setting forth the technical specifications for such Software and included in the Statement of Work.

"**Term**" has the meaning set forth in the preamble.

"**Test Data**" has the meaning set forth in **Section 11.2**.

"**Test Estimates**" has the meaning set forth in **Section 11.2**.

"**Testing Period**" has the meaning set forth in **Section 12.1(b)**.

"**Third Party**" means any Person other than the State or Contractor.

"**Transition Period**" has the meaning set forth in **Section 23.3**

"**Transition Responsibilities**" has the meaning set forth in **Section 23.3**.

"**Unauthorized Removal**" has the meaning set forth in **Section 9.3(b)**.

"**Unauthorized Removal Credit**" has the meaning set forth in **Section 9.3(c)**.

"**User Data**" means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, processed, generated or output by any device, system or network by or on behalf of the State, including any and all works, inventions, data, analyses and other information and materials resulting from any use of the Software by or on behalf of the State under this Contract, except that User Data does not include the Software or data, information or content, including any GUI, audio, visual or

digital or other display or output, that is generated automatically upon executing the Software without additional user input.

"**Warranty Period**" means the ninety (90) calendar-day period commencing on the date of the State's Acceptance of the Software.

"**Work Product**" means all State-specific deliverables that Contractor is required to, or otherwise does, provide to the State under this Contract including but not limited to computer scripts, macros, user interfaces, reports, project management documents, forms, templates, and other State-specific documents and related materials together with all ideas, concepts, processes, and methodologies developed in connection with this Contract whether or not embodied in this Contract.

2. Statements of Work. Contractor shall provide Services and Deliverables pursuant to Statements of Work entered into under this Contract. No Statement of Work shall be effective unless signed by each party's Contract Administrator. The term of each Statement of Work shall commence on the parties' full execution of the Statement of Work and terminate when the parties have fully performed their obligations. The terms and conditions of this Contract will apply at all times to any Statements of Work entered into by the parties and attached as a schedule to this Contract. The State shall have the right to terminate such Statement of Work as set forth in **Section 23**. Contractor acknowledges that time is of the essence with respect to Contractor's obligations under each Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and the Statements of Work (including the Implementation Plan and all Milestone Dates) is strictly required.

2.1 Statement of Work Requirements. Each Statement of Work will include the following:

(a) names and contact information for Contractor's Contract Administrator, Project Manager and Key Personnel;

(b) names and contact information for the State's Contract Administrator, Project Manager and Business Owner;

(c) a detailed description of the Services to be provided under this Contract, including any training obligations of Contractor;

(d) a detailed description of the Software to be provided under this Contract, including the:

(i) version and release number of the Software;

(ii) Business Requirements Specification;

(iii) Technical Specification; and

(iv) a description of the Documentation to be provided;

(e) an Implementation Plan, including all Milestones, the corresponding Milestone Dates and the parties' respective responsibilities under the Implementation Plan;

(f) the due dates for payment of Fees and any invoicing requirements, including any Milestones on which any such Fees are conditioned, and such other information as the parties deem necessary;

(g) disclosure of all Open-Source Components (each identified on a separate exhibit to the Statement of Work), in each case accompanied by such related documents as may be required by this Contract;

(h) description of all liquidated damages associated with this Contract; and

(i) a detailed description of all State Resources required to complete the Implementation Plan.

2.2 Change Control Process. The State may at any time request in writing (each, a "**Change Request**") changes to the Statement of Work, including changes to the Services and Implementation Plan (each, a "**Change**"). Upon the State's submission of a Change Request, the parties will evaluate and implement all Changes in accordance with this **Section 2.2**.

(a) As soon as reasonably practicable, and in any case within twenty (20) Business Days following receipt of a Change Request, Contractor will provide the State with a written proposal for implementing the requested Change ("**Change Proposal**"), setting forth:

(i) a written description of the proposed Changes to any Services or Deliverables;

(ii) an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any additional or modified Services or Deliverables; and (B) the effect of such Changes, if any, on completing any other Services under the Statement of Work;

(iii) any additional State Resources Contractor deems necessary to carry out such Changes; and

(iv) any increase or decrease in Fees resulting from the proposed Changes, which increase or decrease, will reflect only the increase or decrease in time and expenses Contractor requires to carry out the Change.

(b) Within thirty (30) Business Days following the State's receipt of a Change Proposal, the State will by written notice to Contractor, approve, reject, or propose modifications to such Change Proposal. If the State proposes modifications, Contractor must modify and re-deliver the Change Proposal reflecting such modifications, or notify the State of any disagreement, in which event the parties will negotiate in good faith to resolve their disagreement. Upon the State's approval of the Change Proposal or the parties' agreement on all proposed modifications, as the case may be, the parties will execute a written agreement to the Change Proposal ("**Change Notice**"), which Change Notice will be signed by the State's Contract Administrator and will constitute an amendment to the Statement of Work to which it relates; and

(c) If the parties fail to enter into a Change Notice within fifteen (15) Business Days following the State's response to a Change Proposal, the State may, in its discretion:

(i) require Contractor to perform the Services under the Statement of Work without the Change;

(ii) require Contractor to continue to negotiate a Change Notice;

(iii) initiate a Dispute Resolution Procedure; or

(iv) notwithstanding any provision to the contrary in the Statement of Work, terminate this Contract under **Section 23**.

(d) No Change will be effective until the parties have executed a Change Notice. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with the Statement of Work pending negotiation and execution of a Change Notice. Contractor will use its best efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the applicable Change Notice. Each party is responsible for its own costs and expenses of preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e) The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Services as described in this Contract are considered part of the Services and, thus, will not be considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of Non-Conformities discovered in Deliverables prior to their Acceptance by the State or, subsequent to their Acceptance by the State, as necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

(f) Contractor may, on its own initiative and at its own expense, prepare and submit its own Change Request to the State. However, the State will be under no obligation to approve or otherwise respond to a Change Request initiated by Contractor.

3. Software License. Contractor hereby grants to the State and its Authorized Users the right and license to use the Software and Documentation in accordance with the terms and conditions of this Contract and the License Agreement set forth in **Schedule C** (the "**License Agreement**").

4. Open-Source Licenses. Any use hereunder of Open-Source Components shall be governed by, and subject to, the terms and conditions of the applicable open-source license ("**Open-Source License**"). Contractor shall identify and describe in an exhibit to the Statement of Work each of the Approved Open-Source Components of the Software, and include an exhibit attaching all applicable Open-Source Software Licenses or identifying the URL where these licenses are publicly available.

5. Software Implementation.

5.1 Implementation. Contractor will deliver, install, configure, integrate, and otherwise provide and make fully operational the Software on or prior to the applicable Milestone Date in accordance with the criteria set forth in the Statement of Work.

5.2 Site Preparation. Unless otherwise set forth in the Statement of Work, Contractor is responsible for ensuring the relevant Operating Environment is set up and in working order to allow Contractor to deliver and install the Software on or prior to the applicable Milestone Date. Contractor will provide the State with such notice as is specified in the Statement of Work, prior to delivery of the Software to give the State sufficient time to prepare for Contractor's delivery and installation of the Software. If the State is responsible for Site preparation, Contractor will provide such assistance as the State requests to complete such preparation on a timely basis.

6. Hosting. Contractor will maintain the Availability Requirement and the Support Service Level Requirement set forth in the Service Level Agreement attached as **Schedule E** to this Contract.

7. Support Services

7.1 Support Services for Externally Hosted Software. Contractor shall provide the State with the Support Services described in the Service Level Agreement attached as **Schedule E** to this Contract. Such Support Services shall be provided:

(a) Free of charge during the Warranty Period, it being acknowledged and agreed that the License Fee includes full consideration for such Services during such period.

(b) Thereafter, for so long as the State elects to receive Support Services for the Software, in consideration of the State's payment of Support Services Fees in accordance with **Section 16** and the rates set forth in the Pricing Schedule.

8. Data Privacy and Information Security.

8.1 Undertaking by Contractor. Without limiting Contractor's obligation of confidentiality as further described, Contractor is responsible for establishing and maintaining a data privacy and information security program in accordance with the Security and Management Control Outsourcing Standard for Non-Channeler's, including physical, technical, administrative, and organizational safeguards, that is designed to: (a) ensure the security and confidentiality of the State Data; (b) protect against any anticipated threats or hazards to the security or integrity of the State Data; (c) protect against unauthorized disclosure, access to, or use of the State Data; (d) ensure the proper disposal of State Data; and (e) ensure that all Contractor Representatives comply with all of the foregoing. In no case will the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by the State, as required within the most current version of FBI CJIS Security Policy, including, but not limited to, the "Shall Statements." and the Michigan Addendum. In addition Contractor must at all times comply with all applicable State IT policies and standards. Below links are provided for bidder reference.

8.2 https://www.michigan.gov/dtmb/0,5552,7-358-82547_56579_56755---,00.html

Note: Not all applicable PSP's are available publicly. Controlled PSP's applicable to the RFP are available after signing and returning to the State the required Nondisclosure Agreement (NDA) agreement. Failure to return a signed NDA may be grounds for disqualification.

https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

https://www.fbi.gov/file-repository/compact-council-security-and-management-control-outsourcing-standard-for-non-channelers.pdf

https://www.michigan.gov/msp/0,4643,7-123-3493_72291-294063--,00.html

8.3 To the extent that Contractor has access to the State's computer system, Contractor must comply with the State's Acceptable Use Policy, see https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing the State's system. The State reserves the right to terminate Contractor's access to the State's system if a violation occurs.

8.4 Right of Audit by the State. Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the commencement of

Services and from time to time during the term of this Contract. During the providing of Services, on an ongoing basis from time to time and without notice, the State, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program. In lieu of an on-site audit, upon request by the State, Contractor agrees to complete, within forty-five (45) calendar days of receipt, an audit questionnaire provided by the State regarding Contractor's data privacy and information security program.

8.5 Audit Findings. With respect to State Data, Contractor must implement any required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program. Contractor is responsible for all cost due to implementation of any required safeguards identified by the State or by an audit of Contractor's data privacy and information security program.

8.6 State's Right to Termination for Deficiencies. The State reserves the right, at its sole election, to immediately terminate this Contract or the Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this **Section** 8.

8.7 Security Requirements for Externally Hosted Software. If the Operating Environment for the Software is externally hosted by Contractor or a subcontractor, Contractor shall comply with the security requirements set forth in **Schedule F** to this Contract.

9. Performance of Services. Contractor will provide all Services and Deliverables in a timely, professional and workmanlike manner and in accordance with the terms, conditions, and Specifications set forth in this Contract and the Statement of Work. If any of the Contractor personnel resources and responsibilities identified for implementation and on-going support of the solution should change, Contractor is to notify the State's Project Manager and Agency Business Owner in writing, within 3 business days of change. Emailed communication will suffice as "in writing" specifically for this purpose.

9.1 Contractor Personnel.

(a) Contractor is solely responsible for all Contractor Personnel and for the payment of their compensation, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(b) Prior to any Contractor Personnel performing any Services, Contractor will:

(i) Ensure that such Contractor Personnel have the legal right to work in the United States;

(ii) Upon request, require such Contractor Personnel to execute written agreements, in form and substance acceptable to the State, that bind such Contractor Personnel to confidentiality provisions that are at least as protective of the State's information (including all Confidential Information) as those contained in this Contract; and

(iii) Perform state and federal fingerprint-based background checks on all Contractor and Subcontractor Personnel prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks on Contractor Personnel.

(iv) Require all Contractor and Subcontractor Personnel complete Basic security awareness training within six months of initial assignment (or other mutually agreed upon timeframe), and biennially thereafter, for all personnel who have access to MSP SOR data to include all personnel who have unescorted access to a physically secure location. Contractor is to ensure the four levels of security training are provided as applicable to personnel data access, in accordance with the most current version of the FBI CJIS Security Policy.

(i) Require all Contractor and Subcontractor Personnel complete and sign a CJIS Security Addendum and abide by all aspects of the addendum.

(c) Contractor and all Contractor Personnel will comply with all applicable rules, regulations, and policies of the State that are communicated to Contractor in writing, including security procedures concerning systems and data and remote access, building security procedures (while providing on-site services), including the restriction of access by the State to certain areas of its premises or systems, and general health and safety practices and procedures.

(d) The State reserves the right to require the removal of any Contractor Personnel found, in the judgment of the State, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and Contractor cannot immediately replace the removed personnel, the State agrees to negotiate an equitable adjustment in schedule or other terms that may be affected by the State's required removal.

9.2 Contractor's Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to the State to serve as Contractor's Project Manager, who will be considered Key Personnel of Contractor. Contractor's Project Manager will be identified in the Statement of Work.

(a) Contractor's Project Manager must:

(i) have the requisite authority, and necessary skill, experience, and qualifications, to perform in such capacity;

(ii) be responsible for overall management and supervision of Contractor's performance under this Contract; and

(iii) be the State's primary point of contact for communications with respect to this Contract, including with respect to giving and receiving all day-to-day approvals and consents.

(b) Contractor's Project Manager must attend all regularly scheduled meetings as set forth in the Implementation Plan and will otherwise be available as set forth in the Statement of Work.

(c) Contractor will maintain the same Project Manager throughout the Term of this Contract, unless:

(i) the State requests in writing the removal of Contractor's Project Manager;

(ii) the State consents in writing to any removal requested by Contractor in writing;

(iii) Contractor's Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.

(d) Contractor will promptly replace its Project Manager on the occurrence of any event set forth in **Section 9.2(c)**. Such replacement will be subject to the State's prior written approval.

9.3 Contractor's Key Personnel.

(a) The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State's Project Manager, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection. If at any time during the course of the contract a Contractor Key Personnel is determined by the State unfit for their assignment, the State will provide written explanation including reasonable detail outlining its reason for reassignment. Upon receipt of such explanation the Contractor will remove said personnel assignment. The Contractor will assign new Key Personnel, having meet all contractor personnel requirements, within 30 days of written explanation. Any objections or refusals of reassignment may be considered by the State to be a material breach of the Contract, in respect of which the State may elect to terminate this Contract for cause under **Section 23.1.**

(b) Contractor will not remove any Key Personnel from their assigned roles on this Contract without prior written notice to the State. The Contractor's removal of Key Personnel without providing notice to the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract, in respect of which the State may elect to terminate this Contract for cause under **Section 23.1**.

(c) It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of this Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 23.1**, Contractor will issue to the State an amount equal to $25,000 per individual (each, an "**Unauthorized Removal Credit**").

(d) Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **Subsection (c)** above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract.

9.4 Subcontractors. Contractor will not, without the prior written approval of the State, which consent may be given or withheld in the State's sole discretion, engage any Third Party to perform Services. The State's approval of any such Third Party (each approved Third Party, a "**Permitted**

Subcontractor") does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

(a) be responsible and liable for the acts and omissions of each such Permitted Subcontractor (including such Permitted Subcontractor's employees who, to the extent providing Services or Deliverables, shall be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

(b) name the State a third-party beneficiary under Contractor's Contract with each Permitted Subcontractor with respect to the Services;

(c) be responsible for all fees and expenses payable to, by or on behalf of each Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and

(d) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.

10. State Obligations.

10.1 State Resources and Access. The State is responsible for:

(a) providing the State Materials and such other resources as may be specified in the Statement of Work (collectively, "**State Resources**"); and

(b) if the Software is internally hosted on State systems, providing Contractor Personnel with such access to the Site(s) and Operating Environment as is necessary for Contractor to perform its obligations on a timely basis as set forth in the Statement of Work.

10.2 State Project Manager. Throughout the Term of this Contract, the State will maintain a State employee to serve as the State's Project Manager under this Contract. The State's Project Manager will be identified in the Statement of Work. The State's Project Manager will be available as set forth in the Statement of Work.

11. Pre-Delivery Testing.

11.1 Testing By Contractor. Before delivering and installing the Software, Contractor must:

(a) test the Software to confirm that it is fully operable, meets all applicable Specifications and will function in accordance with the Specifications and Documentation when properly installed in the Operating Environment;

(b) scan the Software using industry standard scanning software and definitions to confirm it is free of Harmful Code; and

(c) remedy any Non-Conformity or Harmful Code identified and retest and rescan the Software.

11.2 Test Data and Estimates. Unless otherwise specified in the Statement of Work, Contractor shall provide to the State all test data and testing scripts used by Contractor for its pre-delivery testing ("**Test**

Data"), together with the results Contractor expects to be achieved by processing the Test Data using the Software ("**Test Estimates**," and together with Test Data, "**Contractor's Test Package**").

12. Acceptance Testing.

12.1 Acceptance Testing.

(a) Unless otherwise specified in the Statement of Work, upon installation of the Software, Acceptance Tests will be conducted as set forth in this **Section 12** to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation. The State may, but is not obligated, to perform its own pretest on the Software utilizing Contractor's Test Package. If the State does perform a pretest, and Contractor's Test Package does not successfully pass the Test Data or Test Estimate scripts as described by Contractor, the State, at its discretion, is not obligated to move into the formal Acceptance Tests set forth in this Section. The State may elect to send Contractor's Test Package back to Contractor to correct any problems encountered with the Test Data or Test Estimates.

(b) All Acceptance Tests will take place at the designated Site(s) in the Operating Environment described in the Statement of Work, commence on the Business Day following installation of the Software and be conducted diligently for up to thirty (30) Business Days, or such other period as may be set forth in the Statement of Work (the "**Testing Period**"). Acceptance Tests will be conducted by the party responsible as set forth in the Statement of Work or, if the Statement of Work does not specify, the State, provided that:

(i) for Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and

(ii) for Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such Acceptance Tests.

Contractor is solely responsible for all costs and expenses related to Contractor's performance of, participation in, and observation of Acceptance Testing.

(c) Upon delivery and installation of any API, Configuration or Customization to the Software under the Statement of Work, additional Acceptance Tests will be performed on the modified Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software ("**Integration Testing**"). Integration Testing is subject to all procedural and other terms and conditions set forth in **Section 12.1**, **Section 12.3**, and **Section 12.4**.

(d) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material Non-Conformity in the tested Software or part or feature of the Software. In such event, Contractor will immediately, and in any case within ten (10) Business Days, correct such Non-Conformity, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period.

12.2 Notices of Completion, Non-Conformities, and Acceptance. Within fifteen (15) Business Days following the completion of any Acceptance Tests, including any Integration Testing, the party responsible for conducting the tests will prepare and provide to the other party written notice of the completion of the

tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Non-Conformity in the tested Software.

(a) If such notice is provided by either party and identifies any Non-Conformities, the parties' rights, remedies, and obligations will be as set forth in **Section 12.3** and **Section 12.4**.

(b) If such notice is provided by the State, is signed by the State's Business Owner and Project Manager, and identifies no Non-Conformities, such notice constitutes the State's Acceptance of such Software.

(c) If such notice is provided by Contractor and identifies no Non-Conformities, the State will have thirty (30) Business Days to use the Software in the Operating Environment and determine, in the exercise of its sole discretion, whether it is satisfied that the Software contains no Non-Conformities, on the completion of which the State will, as appropriate:

(i) notify Contractor in writing of Non-Conformities the State has observed in the Software and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in **Section 12.3** and **Section 12.4**; or

(ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by the State's Business Owner and Project Manager.

12.3 Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Non-Conformities and re-deliver the Software, in accordance with the requirements set forth in the Statement of Work. Redelivery will occur as promptly as commercially possible and, in any case, within thirty (30) Business Days following, as applicable, Contractor's:

(a) completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or

(b) receipt of the State's notice under **Section 12.1(a)** or **Section 12.2(c)(i)**, identifying any Non-Conformities.

12.4 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformity in the Software after a second or subsequent delivery of the Software, or Contractor fails to re-deliver the Software on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

(a) continue the process set forth in this **Section 12**;

(b) accept the Software as a nonconforming deliverable, in which case the Fees for such Software will be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or

(c) deem the failure to be a non-curable material breach of this Contract and the Statement of Work and terminate this Contract for cause in accordance with **Section 23.1**.

12.5 Acceptance. Acceptance ("**Acceptance**") of the Software (subject, where applicable, to the State's right to Integration Testing) will occur on the date that is the earliest of the State's delivery of a notice accepting the Software under **Section 12.2(b)**, or **Section 12.2(c)(ii)**.

13. Training. Contractor shall provide, at no additional charge, training on all uses of the Software permitted hereunder in accordance with the times, locations and other terms set forth in the Statement of Work. Upon the State's request, Contractor shall timely provide training for additional Authorized Users or other additional training on all uses of the Software for which the State requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

14. Maintenance Releases; New Versions

14.1 Maintenance Releases. Provided that the State is current on its Support Services Fees, during the Term, Contractor shall provide the State, at no additional charge, with all Maintenance Releases, each of which will constitute Software and be subject to the terms and conditions of this Contract.

14.2 New Versions. Provided that the State is current on its Support Services Fees, during the Term, Contractor shall provide the State, at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

14.3 Installation. The State has no obligation to install or use any Maintenance Release or New Versions. If the State wishes to install any Maintenance Release or New Version, the State shall have the right to have such Maintenance Release or New Version installed, in the State's discretion, by Contractor or other authorized party as set forth in the Statement of Work. Contractor shall provide the State, at no additional charge, adequate Documentation for installation of the Maintenance Release or New Version, which has been developed and tested by Contractor and Acceptance Tested by the State. The State's decision not to install or implement a Maintenance Release or New Version of the Software will not affect its right to receive Support Services throughout the Term of this Contract. The Parties agree that Contractor is not obligated to ensure that its Services are compatible with outdated (exceeding 4 years from date of initial release) hardware, computer operating services or database engines.

15. Source Code Escrow

15.1 Escrow Contract. The parties may enter into a separate intellectual property escrow agreement, which shall be at the expense of the State. Such escrow agreement will govern all aspects of Source Code escrow and release.

16. Fees

16.1 License Fee. In consideration of, and as payment in full for, the rights and license to use the Software and Documentation as provided in this Contract and the License Agreement, the State shall pay to Contractor the license fees (the "**License Fee**") set forth on the Pricing Schedule, subject to and in accordance with the terms and conditions of this Contract and the License Agreement, including the applicable timetable and other provisions of the Statement of Work and this **Section 16**.

16.2 Implementation Fees. In consideration of, and as payment in full for, Contractor's provision of implementation services as provided in this Contract and the Statement of Work, the State shall pay to Contractor the implementation fees (the "**Implementation Fees**") set forth on the Pricing Schedule, subject to and in accordance with the terms and conditions of this Contract, including the applicable timetable and other provisions of the Statement of Work and this **Section 16**.

16.3 Support Service Fees. In consideration of Contractor providing the Support Services as required under the Maintenance and Support Schedule (as applicable) or the Service Level Agreement

(as applicable), the State shall pay to Contractor the Support Services fees (the "**Support Service Fees**") set forth in the Pricing Schedule, subject to and in accordance with the terms and conditions of this Contract, including the applicable provisions of the Maintenance and Support Schedule (as applicable) or the Service Level Agreement (as applicable) and this **Section 16**.

16.4 Firm Pricing/Fee Changes. All Pricing set forth in this Contract is firm and will not be increased, except as otherwise expressly provided in this **Section 16.4**.

(a) The License Fee will not be increased at any time except for the addition of additional licenses, the fees for which licenses will also remain firm in accordance with the Pricing set forth in the Pricing Schedule.

17. Invoices and Payment.

17.1 Invoices. Contractor will invoice the State for Fees in accordance with the requirements set forth in the Statement of Work, including any requirements that condition the rendering of invoices and the payment of Fees upon the successful completion of Milestones. Contractor must submit each invoice in both hard copy and electronic format, via such delivery means and to such address as are specified by the State in the Statement of Work. Each separate invoice must:

(a) clearly identify the Contract and purchase order number to which it relates, in such manner as is required by the State;

(b) list each Fee item separately;

(c) include sufficient detail for each line item to enable the State to satisfy its accounting and charge-back requirements;

(d) for Fees determined on a time and materials basis, report details regarding the number of hours performed during the billing period, the skill or labor category for such Contractor Personnel and the applicable hourly billing rates;

(e) include such other information as may be required by the State as set forth in the Statement of Work; and

(f) Itemized invoices must be submitted to DTMB-Accounts-Payable@michigan.gov.

17.2 Payment. Invoices are due and payable by the State, in accordance with the State's standard payment procedures as specified in 1984 Public Act no. 279, MCL 17.51, et seq., within forty-five (45) calendar days after receipt, provided the State determines that the invoice was properly rendered. The State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State at http://www.michigan.gov/SIGMAVSS to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment

17.3 Taxes. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services or Deliverables purchased under this Contract are for the State's exclusive use. Notwithstanding the foregoing, all Fees are exclusive of taxes.

17.4 Payment Disputes. The State may withhold from payment any and all payments and amounts the State disputes in good faith, pending resolution of such dispute, provided that the State:

(a) timely renders all payments and amounts that are not in dispute;

(b) notifies Contractor of the dispute prior to the due date for payment, specifying in such notice:

(i) the amount in dispute; and

(ii) the reason for the dispute set out in sufficient detail to facilitate investigation by Contractor and resolution by the parties;

(c) works with Contractor in good faith to resolve the dispute promptly; and

(d) promptly pays any amount determined to be payable by resolution of the dispute.

Contractor shall not withhold any Services or fail to perform any obligation hereunder by reason of the State's good faith withholding of any payment or amount in accordance with this **Section 17.4** or any dispute arising therefrom.

17.5 Right of Setoff. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

18. Intellectual Property Rights

18.1 Ownership Rights in Software

(a) Subject to the rights and licenses granted by Contractor in this Contract and the License Agreement, and the provisions of **Section 18.1(b)**:

(i) The State acknowledges and agrees that Contractor has previously developed certain capabilities and functionalities, which comprise the basic framework of public safety solutions created by Contractor ("**Core Framework**"). The State further acknowledges and agrees that the Core Framework will be leveraged by Contractor in connection with the performance of its obligations hereunder.

(ii) For purposes of this Contract, Contractor's Core Framework shall include:

1. Business rules, workflow and document management, data searching, reporting, analytics, mapping, data capture, validation, notification, and redaction tools

2. System workflow and/or administration including database access, auditing, transaction/usage logging, user security and function access control

3. Case/transaction management functionality

4. Web entry/registration application

5. Quality control and processing module, which includes inboxes and work queues for registration processing and

reporting functionality. This also includes the administrator module.

6. Notification and correspondence module.

(i) The Core Framework shall be deemed Contractor's Pre-existing Intellectual Property (as defined above).Contractor reserves and retains its entire right, title and interest in and to all Pre-exiting Intellectual Property Rights arising out of or relating to the Software; and

(ii) none of the State or Authorized Users acquire any ownership of the Pre-existing Intellectual Property Rights in or to the Software or Documentation as a result of this Contract.

(b) As between the State, on the one hand, and Contractor, on the other hand, the State has, reserves and retains, sole and exclusive ownership of all right, title and interest in and to User Data, including all Work Product arising therefrom or relating thereto.

18.2 Rights in Open-Source Components. Ownership of all Intellectual Property Rights in Open-Source Components shall remain with the respective owners thereof, subject to the State's rights under the applicable Open-Source Licenses.

18.3 The State is and will be the sole and exclusive owner of all right, title, and interest in and to all API and Work Product developed exclusively for the State under this Contract, excluding all Pre-existing Intellectual Property Rights. For purposes of this Contract, Work Product, as it relates to the Sex Offender Registry System includes:

(a) User Administration Configuration for user roles and permissions
(b) State-specific interfaces with external State, County, and local systems
(c) State-specific data entry interfaces
(d) Legacy migration/conversion of data
(e) State-specific training material developed under contract

(f) Contractor will create all API and Work Product as work made for hire as defined in Section 101 of the Copyright Act of 1976; and

(g) to the extent any API, Work Product, or Intellectual Property Rights do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

(i) assigns, transfers, and otherwise conveys to the State, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such API or Work Product, including all Intellectual Property Rights; and

(ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called "moral rights" or rights of *droit moral* with respect to the API or Work Product.

For the avoidance of doubt, Contractor retains all right, title and interest under applicable contractual, copyright and related laws to its Pre-existing Intellectual Property. Solely for the purposes permitted under this Contract, Contractor hereby grants the State, a perpetual, non-exclusive license to use Contractor's Pre-existing Intellectual Property in connection with the Sex Offender Registry system. The State shall not

remove or obscure any copyright or other notices from such Pre-existing Intellectual Property or related data and material provided hereunder.

19. State Data.

19.1 Ownership. The State's data ("**State Data**"), which will be treated by Contractor as Confidential Information, includes: (a) User Data; and (b) any other data collected, used, processed, stored, or generated by the State in connection with the Services, including but not limited to (i) personally identifiable information ("**PII**") collected, used, processed, stored, or generated as the result of the Services, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed and (iii) CJI Data. State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State. This **Section** 19.1 survives termination or expiration of this Contract.

19.2 Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Services. Contractor must: (a) keep and maintain State Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) use and disclose State Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with this Contract, any applicable Statement of Work, and applicable law; and (c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. This **Section 19.2** survives termination or expiration of this Contract

19.3 Hosting Security Measures

a. **Data Security Program**. Contractor shall maintain policies and procedures, which it shall review, test and update, as appropriate, covering the administrative, physical and technical safeguards in place and relevant to the access, use, loss, alteration, disclosure, storage, destruction and control of State Data and the Database, and which are measured against objective standards and controls. Contractor's Data security program shall comply with all applicable laws and regulations. Contractor's security program shall meet or exceed industry best practices, ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, and account for known and reasonably anticipated risks and threats, and Contractor shall, on an continuous basis, monitor for new threats. Contractor shall follow its security policies and procedures. Contractor's security program shall be in writing, and at a minimum, address the following areas:

a. Physical security inclusive of ensuring that physical access to facilities is restricted and controlled to allow access only to authorized personnel, and that such physical access is terminated when no longer needed;

a. Access control and management including the identification, authentication and control of access to, and use of, that Data, information, facilities, networks, computers and software including deactivation of credentials when no longer needed;

b. Appropriate logging and monitoring;

c. Virus and malicious software detection, response and eradication performed on a timely basis;

d. Network controls to prevent and detect malicious activities and segregate physical and logical access;

e. Procedures for appropriate retention, handling and destruction of information; and

f. Appropriate backup, disaster recovery and business continuity plans including, for example, the ability to restore the availability and access to Data in a timely manner in the event of a physical or technical incident; and

g. Investigation and communication regarding Data breaches.

b. **Compromise of State Data**. In the event Contractor confirms that PII has been disclosed to an unauthorized party ("Compromise of PII"), Contractor shall, without disclosing information that is protected by a right of attorney-client privilege Contractor may have with its attorney or would otherwise require Contract to breach an independent obligation of confidentiality to another party (for example, another customer):

a. promptly notify State and investigate the situation;

b. upon request, provide a reasonable summary of the circumstances surrounding such compromise of PII to the State;

c. cooperate reasonably with State's requests for information regarding such compromise of PII;

d. bear all costs associated with complying with its legal and regulatory obligations in connection therewith; and

e. with respect to a Compromise of PII resulting from: (i) Contractor's breach of its security obligations as set forth in Section 19.3(a) of this Agreement or (ii) any intentional disclosure by a Contractor employee who is authorized to access PII, be responsible for the legal obligations and any associated costs in connection with a compromise of PII, including, but not limited to: litigation (including attorney's fees); reimbursement sought by individuals (including costs for credit monitoring and other losses alleged to be in connection with such compromise of State Data).

c. **Compliance with Laws**. Additionally, State agrees to comply with all applicable laws and regulations, including those governing the State Data provided to Contractor under this Agreement, and any other applicable data security standards and privacy regulations.

19.4 State's Governance, Risk and Compliance (GRC) platform. Contractor is required to assist the State with its security accreditation process through the development, completion and ongoing updating of a system security plan using the State's automated GRC platform, and implement any required safeguards or remediate any security vulnerabilities as identified by the results of the security accreditation process.

20. Confidential Information. Each party acknowledges that it may be exposed to or acquire communication or data of the other party that is confidential in nature and is not intended to be disclosed to third parties. This **Section 20** survives termination or expiration of this Contract.

20.1 Meaning of Confidential Information. The term "**Confidential Information**" means all information and documentation of a party that: (a) has been marked "confidential" or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked "confidential" or with

words of similar meaning, was subsequently summarized in writing by the disclosing party and marked "confidential" or with words of similar meaning; and, (c) should reasonably be recognized as confidential information of the disclosing party. The term "Confidential Information" does not include any information or documentation that was or is: (a) in the possession of the State and subject to disclosure under the Michigan Freedom of Information Act (FOIA); (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party's proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party). Notwithstanding the above, in all cases and for all matters, State Data is deemed to be Confidential Information.

20.2 Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to the Contractor's subcontractor is permissible where: (a) the subcontractor is a Permitted Subcontractor; (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Permitted Subcontractor's responsibilities; and (c) Contractor obligates the Permitted Subcontractor in a written contract to maintain the State's Confidential Information in confidence. At the State's request, any of the Contractor's Representatives may be required to execute a separate agreement to be bound by the provisions of this **Section 20.2**.

20.3 Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract. Each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

20.4 Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the case of the State, at the sole election of the State, the immediate termination, without liability to the State, of this Contract or any Statement of Work corresponding to the breach or threatened breach.

20.5 Surrender of Confidential Information upon Termination. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within five (5) Business Days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. If Contractor or the State determine that the return of any Confidential Information is not feasible, such party must destroy the Confidential Information and certify the same in writing within five (5) Business Days from the date of termination to the other party.

21. Reserved

22. ADA Compliance. The State is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. Contractor's Service Software must comply, where relevant, with level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.

23. CJIS Compliance. Contractor shall comply with all Criminal Justice Information Services (CJIS) Security Policy requirements that are communicated to the Contractor in writing, including the FBI CJIS Security Addendum attached as **Schedule H**. Changes required to Contractor's performance due to a change in CJIS requirements shall be subject to **Section 2.2 Change Control Process.** The State reserves the right to perform additional background checks on Contractor personnel as may be required to comply with the CJIS Security Policy During the term, Contractor will maintain complete and accurate records relating to its data protection practices and the security of any of the State's Confidential Information, including any backup, disaster recovery or other policies, practices or procedures relating to the State's Confidential Information and any other information relevant to its compliance with this **Section 23**. Contractor shall make all such records, appropriate personnel, and relevant materials available in the event of an audit initiated by the State or the FBI.

24. Termination, Expiration, Transition. The State may terminate this Contract, the Support Services, or any Statement of Work, in accordance with the following:

24.1 Termination for Cause. In addition to any right of termination set forth elsewhere in this Contract:

(a) The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State: (i) endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel; (ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or (iii) breaches any of its material duties or obligations under this Contract. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

(b) If the State terminates this Contract under this **Section 24.1**, the State will issue a termination notice specifying whether Contractor must: (a) cease performance immediately, or (b) continue to perform for a specified period. If it is later determined that Contractor was not in breach of this Contract, the termination will be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 24.2**.

24.2 The State will only pay for amounts due to Contractor for Services accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination, including any prepaid Support Services Fees. Further, Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs.

24.3 Termination for Convenience. The State may terminate this Contract in whole or in part, without penalty and for any reason by providing notice to Contractor of such intent, thirty (30) days prior to the termination effective date. However, the State may immediately terminate this Contract in whole or in part, without penalty for appropriation or budget shortfalls. The termination notice will specify whether

Contractor must: (a) cease performance immediately, or (b) continue to perform in accordance with **Section 23.3**. If the State terminates this Contract for convenience, the State will pay all reasonable costs, as determined by the State, for State approved Transition Responsibilities to the extent the funds are available.

24.4 Transition Responsibilities. Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days; the "**Transition Period**"), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the State or its designees. Such transition assistance may include but is not limited to: (a) continuing to perform the Services at the established Contract rates; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services to the State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return to the State all State Data; and (d) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the "**Transition Responsibilities**"). The Term of this Contract is automatically extended through the end of the Transition Period.

24.5 Survival. The following **Sections 8, 18, 19, 20, 23, 24, 28, 29, 32.5, 32.11** survive termination or expiration of this Contract.

25. Stop Work Order. The State may, at any time, order the Services of Contractor fully or partially stopped for its own convenience for up to ninety (90) calendar days at no additional cost to the State. The State will provide Contractor a written notice detailing such suspension (a "**Stop Work Order**"). Contractor must comply with the Stop Work Order upon receipt. Within 90 days, or any longer period agreed to by Contractor, the State will either: (a) issue a notice authorizing Contractor to resume work, or (b) terminate this Contract. The State will not pay for any Services, Contractor's lost profits, or any additional compensation during a stop work period.

26. Contractor Representations and Warranties.

26.1 Authority. Contractor represents and warrants to the State that:

(a) It is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Contract under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;

(b) It has the full right, power, and authority to enter into this Contract, to grant the rights and licenses granted under this Contract, and to perform its contractual obligations;

(c) The execution of this Contract by its Representative has been duly authorized by all necessary organizational action; and

(d) When executed and delivered by Contractor, this Contract will constitute the legal, valid, and binding obligation of Contractor, enforceable against Contractor in accordance with its terms.

26.2 Bid Response. Contractor represents and warrants to the State that:

(a) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other Bidder for the purpose of restricting competition; the prices

quoted were not knowingly disclosed by Contractor to any other Bidder to the Direct Solicitation; and no attempt was made by Contractor to induce any other Person to submit or not submit a proposal for the purpose of restricting competition;

(b) All written information furnished to the State by or for Contractor in connection with this Contract, including Contractor's Bid Response, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading;

(c) Contractor is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State within the previous five (5) years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract; and

(d) If any of the certifications, representations, or disclosures made in Contractor's Bid Response change after contract award, the Contractor is required to report those changes immediately to the Contract Administrator.

26.3 Software Representations and Warranties. Contractor further represents and warrants to the State that:

(a) it is the legal and beneficial owner of the entire right, title and interest in and to the Software, including all Intellectual Property Rights relating thereto;

(b) it has, and throughout the license term, will retain the unconditional and irrevocable right, power and authority to grant and perform the license hereunder;

(c) the Software, and the State's use thereof, is and throughout the license term will be free and clear of all encumbrances, liens and security interests of any kind;

(d) neither its grant of the license, nor its performance under this Contract does or to its knowledge will at any time:

(i) conflict with or violate any applicable Law;

(ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or

(iii) require the provision of any payment or other consideration to any third party;

(e) when used by the State or any Authorized User in accordance with this Contract and the Documentation, the Software or Documentation as delivered or installed by Contractor does not or will not:

(i) infringe, misappropriate or otherwise violate any Intellectual Property Right or other right of any third party; or

(ii) fail to comply with any applicable Law;

(f) as provided by Contractor, the Software does not or will not at any time during the license term contain any:

(i) Harmful Code; or

(ii) Open-Source Components or operate in such a way that it is developed or compiled with or linked to any Open-Source Components, other than Approved Open-Source Components specifically described in the Statement of Work.

(g) all Documentation is and will be complete and accurate in all material respects when provided to the State such that at no time during the license term will the Software have any material undocumented feature; and

(h) it will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract.

(i) when used in the Operating Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with this Contract and the Documentation; and

(j) no Maintenance Release or New Version, when properly installed in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.

26.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THIS CONTRACT.

27. Indemnification

27.1 General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all third party actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), ("Claims") arising out of or relating to Contractor's (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable): (a) a violation of laws in the performance of its obligations contained in this Contract; (b) breach of its security and notification obligations as set forth in Section 19.3. (Hosting Security Measures) (c) breach of the confidentiality obligations set forth in Section 20, Confidential information, herein; (d) infringement, misappropriation, or other violation of any U.S. Intellectual Property Right or other right of any Third Party; and (e) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

27.2 Indemnification Procedure. The State will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor must, to the satisfaction of the State, demonstrate its financial ability to carry out these obligations. The State is entitled to: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; and (iii) employ its own counsel; and to (iv) retain control of the defense, at its own cost and expense, if the State deems necessary, in such case, Contractor shall be relieved of its indemnification obligations hereunder. Contractor will not, without the State's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in

or otherwise seek to terminate any claim, action, or proceeding. Any litigation activity on behalf of the State or any of its subdivisions, under this **Section 26**, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

27.3 Infringement Remedies.

(a) The remedies set forth in this **Section 26.3** are in addition to, and not in lieu of, all other remedies that may be available to the State under this Contract or otherwise, including the State's right to be indemnified for such actions.

(b) If any Software or any component thereof, other than State Materials, is found to be infringing or if any use of any Software or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an infringement claim, Contractor must, at Contractor's sole cost and expense:

(i) procure for the State the right to continue to use such Software or component thereof to the full extent contemplated by this Contract; or

(ii) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Software and all of its components non-infringing while providing fully equivalent features and functionality.

(c) If neither of the foregoing is possible notwithstanding Contractor's best efforts, then Contractor may direct the State to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Contractor will:

(i) refund to the State all amounts paid by the State in respect of such Allegedly Infringing Materials and any other aspects of the Software provided under the Statement of Work for the Allegedly Infringing Materials that the State cannot reasonably use as intended under this Contract; and

(ii) in any case, at its sole cost and expense, secure the right for the State to continue using the Allegedly Infringing Materials for a transition period of up to six (6) months to allow the State to replace the affected features of the Software without disruption.

(d) If Contractor directs the State to cease using any Software under **subsection (c)**, the State may terminate this Contract for cause under **Section 23.1**.

(e) Contractor will have no liability for any claim of infringement arising solely from:

(i) Contractor's compliance with any designs, specifications, or instructions of the State; or

(ii) modification of the Software by the State without the prior knowledge and approval of Contractor;

unless the claim arose against the Software independently of any of the above specified actions.

28. Damages Disclaimers and Limitations.

28.1 The State's Disclaimer of Damages. THE STATE WILL NOT BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

28.2 The State's Limitation of Liability. IN NO EVENT WILL THE STATE'S AGGREGATE LIABILITY TO CONTRACTOR UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE MAXIMUM AMOUNT OF FEES PAYABLE UNDER THIS CONTRACT.

28.3 The Contractor's Limitation of Liability and disclaimer of damages. To the extent permitted by applicable law, Contractor's liability to the State under this Contract, regardless of the form of action, whether in contract, tort, negligence, strict liability or by statute or otherwise, for any claim, including negligence claims, under this Contract shall not exceed THREE MILLION EIGHT HUNDRED THOUSAND DOLLARS ($3,800,000.00) per occurrence. NOTWITHSTANDING THE FOREGOING, CONTRACTOR'S MAXIMUM LIABILITY TO THE STATE UNDER THIS CONTRACT SHALL NOT EXCEED NINE MILLION NINE HUNDRED NINETY-NINE THOUSAND NINE HUNDRED NINETY-NINE DOLLARS AND NINETY-NINE CENTS ($9,999,999.99) IN THE AGGREGATE OVER THE TERM OF THE CONTRACT. The foregoing limitations of liability shall not apply to Contractor's indemnification obligation for third party claims arising out of any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor as set forth in subsection 27.1(e) or any claims, actions, damages, liabilities or fines relating to or arising from Contractor's gross negligence or willful misconduct.

IN NO EVENT SHALL CONTRACTOR BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THIS CONTRACT OR THE PERFORMANCE OR FAILURE TO PERFORM HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

29. Records Maintenance, Inspection, Examination, and Audit.

Right of Audit. The State or its designee may audit Contractor, to verify compliance with this Contract. Contractor must retain and provide to the State or its designee and the auditor general upon request, all financial and accounting records related to this Contract through the Term of this Contract and for four (4) years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Financial Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Financial Audit Period, Contractor must retain the records until all issues are resolved.

29.1 Right of Inspection. Within ten (10) calendar days of providing notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor's premises or any other places where Services are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. The State agrees to abide by all security policies and other applicable policies of Contractor in conducting such audits. If financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of this Contract must be paid or refunded within forty-five (45) calendar days.

29.2 Application. This **Section 29** applies to Contractor, any Affiliate, and any Permitted Subcontractor that performs Services in connection with this Contract.

30. Insurance

30.1 Required Coverage.

(a) **Insurance Requirements.** Contractor must maintain the insurances identified below and is responsible for all deductibles. All required insurance must: (a) protect the State from claims that may arise out of, are alleged to arise out of, or result from Contractor's or a subcontractor's performance; (b) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (c) be provided by a company with an A.M. Best rating of "A" or better and a financial size of VII or better.

Insurance Type	Additional Requirements
Commercial General Liability Insurance	
Minimal Limits: $1,000,000 Each Occurrence Limit $1,000,000 Personal & Advertising Injury Limit $2,000,000 General Aggregate Limit $2,000,000 Products/Completed Operations Deductible Maximum: $50,000 Each Occurrence	Contractor must have their policy endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds using endorsement CG 20 10 11 85, or both CG 2010 07 04 and CG 2037 07 0.
Umbrella or Excess Liability Insurance	
Minimal Limits: $5,000,000 General Aggregate	Contractor must have their policy endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds.
Automobile Liability Insurance	
Minimal Limits: $1,000,000 Per Occurrence	
Workers' Compensation Insurance	

Insurance Type	Additional Requirements
Minimal Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimal Limits: $500,000 Each Accident $500,000 Each Employee by Disease $500,000 Aggregate Disease.	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimal Limits: $1,000,000 Each Occurrence $1,000,000 Annual Aggregate	Contractor must have their policy: (1) endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds; and (2) cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.
Crime Insurance	
Minimal Limits: $1,000,000 Employee Theft Per Loss	Contractor must have their policy: (1) cover forgery and alteration, theft of money and securities, robbery and safe burglary, computer fraud, funds transfer fraud, money order and counterfeit currency, and (2) endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as Loss Payees.
Professional Liability (Errors and Omissions) Insurance	

Insurance Type	Additional Requirements
Minimal Limits: $3,000,000 Each Occurrence $3,000,000 Annual Aggregate Deductible Maximum: $50,000 Per Loss	

(b) If Contractor's policy contains limits higher than the minimum limits, the State is entitled to coverage to the extent of the higher limits. The minimum limits are not intended and may not be construed to limit any liability or indemnity of Contractor to any indemnified party or other persons.

(c) If any of the required policies provide claim-made coverage, the Contractor must: (a) provide coverage with a retroactive date before the effective date of the contract or the beginning of contract work; (b) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the contract of work; and (c) if coverage is canceled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the contract effective date, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

(d) Contractor must: (a) provide insurance certificates to the Contract Administrator, containing the agreement or purchase order number, at Contract formation and within 20 calendar days of the expiration date of the applicable policies; (b) require that subcontractors maintain the required insurances contained in this Section; (c) notify the Contract Administrator within 5 business days if any insurance is cancelled; and (d) waive all rights against the State for damages covered by insurance. Failure to maintain the required insurance does not limit this waiver.

30.2 Non-waiver. This **Section 30** is not intended to and is not be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

31. Dispute Resolution.

31.1 Unless otherwise specified in the Statement of Work, the parties will endeavor to resolve any Contract dispute in accordance with **Section 31** (the "**Dispute Resolution Procedure**"). The initiating party will reduce its description of the dispute to writing (including all supporting documentation) and deliver it to the responding party's Project Manager. The responding party's Project Manager must respond in writing within five (5) Business Days. The initiating party has five (5) Business Days to review the response. If after such review resolution cannot be reached, both parties will have an additional five (5) Business Days to negotiate in good faith to resolve the dispute. If the dispute cannot be resolved within a total of fifteen (15) Business Days, the parties must submit the dispute to the parties' Contract Administrators. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance.

31.2 Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' Contract Administrators, and either Contract Administrator concludes that resolution is unlikely, or fails to respond within fifteen (15) Business Days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This **Section 31** does not limit the State's right to terminate this Contract.

32. General Provisions

32.1 Force Majeure.

(a) Force Majeure Events. Subject to **Subsection (b)** below, neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached this Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of this Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure**"), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

(b) State Performance; Termination. In the event of a Force Majeure Event affecting Contractor's performance under this Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate this Contract by written notice to Contractor if a Force Majeure Event affecting Contractor's performance hereunder continues substantially uninterrupted for a period of five (5) Business Days or more. Unless the State terminates this Contract pursuant to the preceding sentence, any date specifically designated for Contractor's performance under this Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

32.2 Further Assurances. Each party will, upon the reasonable request of the other party, execute such documents and perform such acts as may be necessary to give full effect to the terms of this Contract.

32.3 Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Contract is to be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment or fiduciary relationship between the parties, and neither party has authority to contract for or bind the other party in any manner whatsoever.

32.4 Media Releases. News releases (including promotional literature and commercial advertisements) pertaining to this Contract or project to which it relates must not be made without the prior written approval of the State, and then only in accordance with the explicit written instructions of the State.

32.5 Notices. All notices, requests, consents, claims, demands, waivers and other communications under this Contract must be in writing and addressed to the parties as follows (or as otherwise specified by a party in a notice given in accordance with this **Section 32.5**):

If to Contractor:	1000 Alderman Drive	
	Alpharetta, GA 30005	
	Email:	Robert.holtgrave@lexisnexisrisk.com
	Attention:	Robert Holtgrave
If to State:	525 W Allegan St.	
	Lansing, MI 48913	
	Email:	regans@michigan.gov
	Attention:	Sean Regan

Notices sent in accordance with this **Section 32.5** will be deemed effectively given: (a) when received, if delivered by hand (with written confirmation of receipt); (b) when received, if sent by a nationally recognized overnight courier (receipt requested); (c) on the date sent by e-mail (with confirmation of transmission), if sent during normal business hours of the recipient, and on the next Business Day, if sent after normal business hours of the recipient; or (d) on the fifth (5th) day after the date mailed, by certified or registered mail, return receipt requested, postage prepaid.

32.6 Headings. The headings in this Contract are for reference only and do not affect the interpretation of this Contract.

32.7 Assignment. Contractor may not assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance, under this Contract, in each case whether voluntarily, involuntarily, by operation of law or otherwise, without the State's prior written consent. The State has the right to terminate this Contract in its entirety or any Services or Statements of Work hereunder, pursuant to **Section 23.1**, if Contractor delegates or otherwise transfers any of its obligations or performance hereunder, whether voluntarily, involuntarily, by operation of law or otherwise, and no such delegation or other transfer will relieve Contractor of any of such obligations or performance. For purposes of the preceding sentence, and without limiting its generality, any merger, consolidation or reorganization involving Contractor (regardless of whether Contractor is a surviving or disappearing entity) will be deemed to be a transfer of rights, obligations, or performance under this Contract for which the State's prior written consent is required. Any purported assignment, delegation, or transfer in violation of this **Section 32.7** is void.

32.8 No Third-party Beneficiaries. This Contract is for the sole benefit of the parties and their respective successors and permitted assigns. Nothing herein, express or implied, is intended to or will

confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Contract.

32.9 Amendment and Modification; Waiver. No amendment to or modification of this Contract is effective unless it is in writing, identified as an amendment to this Contract and signed by both parties Contract Administrator. Further, certain amendments to this Contract may require State Administrative Board Approval. No waiver by any party of any of the provisions of this Contract will be effective unless explicitly set forth in writing and signed by the party so waiving. Except as otherwise set forth in this Contract, no failure to exercise, or delay in exercising, any right, remedy, power, or privilege arising from this Contract will operate or be construed as a waiver. Nor will any single or partial exercise of any right, remedy, power or privilege under this Contract preclude the exercise of any other right, remedy, power or privilege.

32.10 Severability. If any term or provision of this Contract is invalid, illegal or unenforceable in any jurisdiction, such invalidity, illegality or unenforceability will not affect any other term or provision of this Contract or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal or unenforceable, the parties hereto will negotiate in good faith to modify this Contract so as to affect the original intent of the parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

32.11 Governing Law. This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles.

32.12 Equitable Relief. Each party to this Contract acknowledges and agrees that (a) a breach or threatened breach by such party of any of its obligations under this Contract may give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy and (b) in the event of a breach or a threatened breach by such party of any such obligations, the other party hereto is, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, entitled to equitable relief, including a temporary restraining order, an injunction, specific performance and any other relief that may be available from a court of competent jurisdiction, without any requirement to post a bond or other security, and without any requirement to prove actual damages or that monetary damages will not afford an adequate remedy. Each party to this Contract agrees that such party will not oppose or otherwise challenge the appropriateness of equitable relief or the entry by a court of competent jurisdiction of an order granting equitable relief, in either case, consistent with the terms of this **Section 32.12**.

32.13 Nondiscrimination. Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq*., the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq*., and Executive Directive 2019-09, Vendor and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex (as defined in Executive Directive 2019-09), height, weight, marital status, partisan considerations, any mental or physical disability, or genetic information that is unrelated to the person's ability to perform the duties of a particular job or position. Breach of this covenant is a material breach of the Contract.

32.14 Unfair Labor Practice. Under MCL 423.324, the State may void any Contract with a Contractor or Permitted Subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.

32.15 Schedules All Schedules that are referenced herein and attached hereto are hereby incorporated by reference.

32.16 Counterparts. This Contract may be executed in counterparts, each of which will be deemed an original, but all of which together are deemed to be one and the same agreement and will become effective and binding upon the parties as of the Effective Date at such time as all the signatories hereto have signed a counterpart of this Contract. A signed copy of this Contract delivered by facsimile, e-mail or other means of electronic transmission (to which a signed copy is attached) is deemed to have the same legal effect as delivery of an original signed copy of this Contract.

32.17 Effect of Contractor Bankruptcy. All rights and licenses granted by Contractor under this Contract are and will be deemed to be rights and licenses to "intellectual property," and all Software and Deliverables are and will be deemed to be "embodiments" of "intellectual property," for purposes of, and as such terms are used in and interpreted under, Section 365(n) of the United States Bankruptcy Code (the "**Code**"). If Contractor or its estate becomes subject to any bankruptcy or similar proceeding, the State retains and has the right to fully exercise all rights, licenses, elections, and protections under this Contract, the Code and all other applicable bankruptcy, insolvency, and similar Laws with respect to all Software and other Deliverables. Without limiting the generality of the foregoing, Contractor acknowledges and agrees that, if Contractor or its estate shall become subject to any bankruptcy or similar proceeding:

(a) all rights and licenses granted to the State under this Contract will continue subject to the terms and conditions of this Contract, and will not be affected, even by Contractor's rejection of this Contract; and

(b) the State will be entitled to a complete duplicate of (or complete access to, as appropriate) all such intellectual property and embodiments of intellectual property comprising or relating to any Software or other Deliverables, and the same, if not already in the State's possession, will be promptly delivered to the State, unless Contractor elects to and does in fact continue to perform all of its obligations under this Contract.

32.18 Compliance with Laws. Contractor and its Representatives must comply with all Laws in connection with this Contract.

32.19 Non-Exclusivity. Nothing contained in this Contract is intended nor is to be construed as creating any requirements contract with Contractor. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Services from other sources.

32.20 Card Industry Data Security Standard

a. Undertaking by Contractor. Contractors that process, transmit, store or affect the security of credit/debit cardholder data, must adhere to the Payment Card Industry Data Security Standard (PCI DSS). The Contractor is responsible for the security of cardholder data in its possession. The data may only be used to assist the State or for other uses specifically authorized by law.

b. Cooperation to Notify of Breach. The Contractor must notify the State's Contract Administrator, within 48 hours of discovery, of any breaches in security where cardholder data has been

compromised. In that event, the Contractor must provide full cooperation to the card associations (e.g. Visa, MasterCard, and Discover) and state acquirer representative(s), or a PCI approved third party, to conduct a thorough security review. The review must validate compliance with the PCI Data Security Standard for protecting cardholder data. The Contractor must provide, at the request of the State, the results of such third party security review. At the State's sole discretion, the State may perform its own security review, either by itself or through a PCI approved third party.

c. Responsibilities for Costs Incurred. The Contractor is responsible for all costs incurred as the result of the breach. Costs may include, but are not limited to, fines/fees for non-compliance, card reissuance, credit monitoring, and any costs associated with a card association, PCI approved third party, or State initiated security review. Without limiting Contractor's obligations of indemnification as further described in this Contract, Contractor must indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the breach.

d. Disposing of Cardholder Data. The Contractor must dispose of cardholder data when it is no longer needed in compliance with PCI DSS policy. The Contractor must continue to treat cardholder data as confidential upon contract termination.

e. Audit by Contractor. The Contractor must provide the State's Contract Administrator with an annual Attestation of Compliance or a Report on Compliance showing the contractor is in compliance with the PCI Data Security Standard. The Contractor must notify the State's Contract Administrator of all failures to comply with the PCI Data Security Standard.

32.21 CEPAS Electronic Receipt Processing Standard

All electronic commerce applications that allow for electronic receipt of credit or debit card and electronic check transactions must be processed via the State's Centralized Electronic Payment Authorization System (CEPAS). To minimize the risk to the State, full credit/debit card numbers, sensitive authentication data, and full bank account information must never be stored on state-owned IT resources.

32.22 Entire Agreement. This Contract, together with all Schedules, Exhibits, and the Statement of Work constitutes the sole and entire agreement of the parties to this Contract with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, representations and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Contract, the Schedules, Exhibits, and the Statement of Work, the following order of precedence governs: (a) first, this Contract, excluding its Exhibits and Schedules, and the Statement of Work; and (b) second, the Statement of Work as of the Effective Date; and (c) third, the Exhibits and Schedules to this Contract as of the Effective Date. NO TERMS ON CONTRACTORS INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE OR ANY AUTHORIZED USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE AND THE AUTHORIZED USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

Schedule A - Statement of Work

1. DEFINITIONS

The following terms have the meanings set forth below. All initial capitalized terms that are not defined below shall have the respective meanings given to them in Section 1 of the Contract Terms and Conditions. "Solution" means the Commercial-Off-the-Shelf (COTS) solution that the State is seeking under this Contract.

Term	Definition
CHR	Criminal History Record
CJIC	Criminal Justice Information Center
EAICS	Electronic Automated Incident Capturing System
FBOP	Federal Bureau of Prisons
ICE	Immigration and Custom Enforcement
LEIN	Law Enforcement Information Network
LSOR	Law Enforcement Sex Offender Registry
MDOC	Michigan Dept. of Corrections
MDHHS	Michigan Dept. of Health and Human Services
MiCars	Michigan Cashiering and Receiving System
MiCJIN	Michigan's Criminal Justice Information Network
NCIC	National Crime Information Center
MSP	Michigan State Police
NSOPW	National Sex Offender Public Website
PMBoK	Project Management Book of Knowledge
OMNI-GEN	OMNI-GEN (Data Integration Platform)
SAML	Security Assertion Markup Language
SNAP	Statewide Network of Agency Photos
SOM	State of Michigan
SOR	Sex Offender Registry
SSO	Single Sign-on

2. BACKGROUND

The Michigan State Police (MSP), Sex Offender Registry (SOR) Unit is responsible for sex offender registration and maintenance of the central repository of sex offender information in Michigan. The SOR database contains the records of approximately 63,000 offenders. It is the SOR Unit's duty to ensure and maintain the accuracy, and detail, of the data housed within the SOR application. This includes keeping the public informed in regards to published offenders, as well as safeguarding the privacy of unpublished offenders. Law enforcement, including but not limited to the Sex Offender Enforcement Unit, is highly dependent on the data that is housed within this repository as they are tasked with tracking and monitoring those who are registered on SOR. Data inaccuracy, or the delayed release of information could be detrimental to public safety and/or a liability for the MSP.

3. PURPOSE

The goal of this project is to implement an externally hosted solution using a FedRAMP-compliant third-party cloud service provider, such as Microsoft Azure or Amazon Web Services (AWS) for a reliable/core SOR system, utilized by all Michigan law enforcement agencies to manage the sex offender population and meet the requirements of federal and state laws. This system needs to be flexible enough to meet the needs and requirements of the registering agencies in the management of their registered sex offenders, while also ensuring the security and integrity of the information and processes.

The state requires a highly configurable/highly adaptive software program - able to be modified without deferment in order to fit any changes mandated by the court and/or impending legislation.
The following is a list of some of the needs that have been identified in regards to a SOR product:

- User and Technical help desk support.
- Application training options, including documentation and materials.
- Automated SOR "Failed To Verify", which identifies those registrants that did not verify within their verification period.
- Billing – Yearly billing of offender $50 registration fee with a cap of $550 per registered offender.
- Interface with various state programs (CHR, SNAP, MiCars, LEIN, OMNI-GEN, etc.).
- A mobile compatible public website.
- Provide allowable data to the public facing site.
- School safety zone mapping.
- Interactive mapping (Sweep Wizard for Enforcement).
- Record auditing.
- A configurable and customizable reporting tool that allows free-form reporting ability for identified administrative users.
- Compatibility with current signature pad software.
- Auto-tiering (when tiering is applicable).
- Ability to store documents.

4. CONTRACT TERM
The contract overall term is to be 5 years, with 2 - 1 Year Options to be used at the discretion of the MSP.

5. SPECIFIC STANDARDS
IT Policies, Standards and Procedures (PSP)
Contractors are advised that the State has methods, policies, standards and procedures that have been developed over the years. Contractors are expected to provide proposals that conform to State IT policies and standards. All services and products provided as a result of this Contract must comply with all applicable State IT policies and standards. Contractor is required to review all applicable links provided below and state compliance in their response.
Public IT Policies, Standards and Procedures (PSP):
https://www.michigan.gov/dtmb/0,5552,7-358-82547_56579_56755---,00.html

Application Scanning
Contractor is required to grant the right to the State to scan either the application code or a deployed version of the solution; or in lieu of the State performing a scan, Contractor will provide the State a vulnerabilities assessment after Contractor has used a State approved application scanning tool. These scans must be completed and provided to the State on a regular basis or at least for each major release.

For COTS or Contractor owned applications, Contractor, at its sole expense, must provide resources to complete the scanning and to complete the analysis, remediation and validation of vulnerabilities identified by the scan as required by the State Secure Web Application Standards.

Application scanning and remediation must include the following types of scans and activities

- Dynamic Application Security Testing (DAST) - Scanning interactive application for vulnerabilities, analysis, remediation and validation (May include IAST)
- Static Application Security Testing (SAST) - Scanning source code for vulnerabilities, analysis, remediation and validation

Application scanning and remediation may include the following types of scans and activities as required based on data classification and/or composition

- Software Composition Analysis (SCA) - Third Party and/or Open Source Scanning for vulnerabilities, analysis, remediation and validation
- Native mobile application software scanning (if applicable) including any interaction with an Application Programming Interface (API)
- Penetration Testing - Simulated attack on the application and infrastructure to identify security weaknesses

Infrastructure Scanning
A Contractor providing Hosted Services must scan the infrastructure using an approved scanning tool (Qualys, Tenable, or other PCI Approved Vulnerability Scanning Tool) at least once every 30 days and provide the scan's assessment to the State in a format that can be uploaded by the State and used to track the remediation. Remediation time frame requirements are documented in SOM PSP's.

Acceptable Use Policy
To the extent that Contractor has access to the State's computer system, Contractor must comply with the State's Acceptable Use Policy, see https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing the State's system. The State reserves the right to terminate Contractor's access to the State's system if a violation occurs.

Look and Feel Standard
All software items provided by the Contractor must adhere to the Look and Feel Standards http://www.michigan.gov/som/0,4669,7-192-86761---,00.html.

Mobile Responsiveness
The Contractor's Solution must utilize responsive design practices to ensure the application is accessible via a mobile device. Contractor's solution is "platform-agnostic" – inherently, there are not any features available via one platform that cannot be performed via a mobile device.

API
The Contractor's solution must include a RESTful Web Service that returns all data in JSON format. Additionally, the two search functions (search by name and search by location) will need to accept the search data provided by the user and return results based on that data. For the search by location, our preference is to use Google Places to geocode the coordinates that are returned to our application.

ADA Compliance
The State is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. The State is requiring that Contractor's Solution, where relevant, to level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0. Contractor may consider, where relevant, the W3C's Guidance on Applying WCAG 2.0 to Non-Web Information and Communications Technologies (WCAG2ICT) for non-web software and content. The State may require that Contractor complete a Voluntary Product Accessibility Template for WCAG 2.0 (WCAG 2.0 VPAT) or other comparable document for the proposed Solution.
http://www.michigan.gov/documents/dmb/1650.00_209567_7.pdf?20151026134621

6. USER TYPE AND CAPACITY

Type of User	Access Type	Number of Users	Number of Concurrent Users in a Day

Public Citizens	Read Only	9.99 million	5,000
MSP SOR Employees	Super Admin Access	2-4	2-4
MSP SOR & SOR Enforcement Employees	Admin Access	16	16
MSP Employees Local Law Enforcement MDOC	Write Access	7,000	7,000
Court Employees Tribal Law Enforcement County Prosecutors MDOC	Read Only Access	1,000	1,000

Contractor will design the application to meet and exceed these expected numbers of concurrent and total users.

7. ACCESS CONTROL AND AUDIT

Contractor's solution must support Identity Federation/Single Sign-on (SSO) capabilities using SAML or comparable mechanisms. The Contractor must already have this configured and running.

To manage users and data, authorized administrators can leverage web-based user administration, workflow, and quality control modules. User administrators are able to define users, user groups, security, and assign permissions to features and functionality. Authorized users can also access records for review, processing and supplementing

Coplogic solution logs all activities that occur within the system, whether that activity is performed by a user or the system itself. For example, the system tracks information that was changed and the identity of the user who made the changes. Changes are timestamped. Authorized administrative users can view a detailed audit/activity log that shows user activity within a specified timeframe.

- Must maintain FedRAMP authorization or an annual SSAE 18 SOC 2 Type 2 audit based on NIST moderate controls for the Solution.

8. DATA RETENTION

Sex Offender File	These records document each registered sex offender. The information is collected in accordance with 42 USC 1407 and Public Act 295 of 1994. The files may include a Sex Offender Registration Form (DD-4), Explanation of Duties to Register as a Sex Offender (DD-4A), Public Sex Offender Registry (PSOR) - Request for Assistance Form, out of state registration, police reports, court documents, death certificates, citizen correspondence, postal service records, out of state drivers' information, etc.	RETAIN UNTIL: Death certificate or police report is received to confirm the death of a sex offender PLUS: 25 years THEN: Destroy

Law Enforcement Sex Offender Registry (LSOR) Data (Any public and non-public data that is maintained within the SOR.)	These records document registered sex offenders, in compliance with Federal regulations. This information is provided to law enforcement agencies using LEIN and to Federal databases. Data may include name, birth date, physical characteristics, address, identification number, conviction information, adjudicated juveniles, out of state offenders, social security number, drivers' license number, state and federal identification numbers, prison information, DNA, etc. This information is collected in accordance with 42 USC 14701, and is exempt from public disclosure.	RETAIN UNTIL: Death certificate or police report is received to confirm the death of a sex offender THEN: Destroy
Public Sex Offender Registry (PSOR) Data	These records document registered sex offenders and are used to notify the public in compliance with Federal regulations (42 USC 14701). Data may include name, birth date, physical characteristics, address, system identification number, conviction information, prison information.	RETAIN UNTIL: Death certificate or police report is received to confirm the death of a sex offender THEN: Destroy

9. SECURITY

Externally Hosted

The Solution will be storing sensitive data.

Contractor will comply with the following:

- Must enter into and sign an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice information.
- Must sign the FBI Criminal Justice Information Services (CJIS) Security Addendum and maintain compliance with such document.
- Must comply with all of the FBI CJIS Security Policy, Version 5.6, and any future versions. https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center, including, but not limited to, the "Shall Statements."
- Must comply with the Michigan Administrative Rules and Michigan Addendums, and any future versions. https://www.michigan.gov/msp/0,4643,7-123-3493_72291-294063--,00.html
- When data is transmitted outside the boundary of a deemed physically secure location, the data shall be encrypted. The cryptographic module used shall be FIPS PUB 140-2 **certified** and use a symmetric cipher key length of at least 128-bits.
- When data is at rest outside the boundary of a deemed physically secure location, the data shall be encrypted. The cryptographic module used shall be FIPS PUB 140-2 **certified** and use a symmetric cipher key length of at least 256-bits
  - Must remain complaint with the Payment Card Industry Data Security Standard (PCI DSS) Policies.
- Must provide a GovCloud Solution that is hosted in a FedRAMP authorized environment/facility.

10. END USER OPERATING ENVIRONMENT

Applications and data developed or purchased by the MSP shall be replicated to the department's Data Hub. By hosting the solution, the Contractor must ensure the data can interface with the Data Hub. DTMB developers, vendors, and contractors required to building applications or house data will be provided the following upon a signed non-disclosure agreement: detailed specifications for the MSP's Data Hub, the MSP's Law Enforcement Data Model, and MSP's native toolset listing.

The MSP's Data Hub Environment consists of four major components which are outlined below.			
The MSP Data Integration Platform:	An MSP toolset made up of software and hardware designed to establish interoperability between disparate systems and data. These include but are not limited to 1) hybrid Hadoop clusters, 2) multiple external and internal application programming interfaces (API's), 3) multiple Extract, Transform, Load (ETL) process, 4) Enterprise Application Integration (EAI) routines, and 5) Enterprise Information Integration (EII) (data virtualization) tools all designed to aggregate heterogeneous data from disparate sources and view it in a consistent manner from a single point of access.		
The MSP Data Quality Routine:	Real-time data standardization, cleansing, and remediation routines. These consist of data-quality routines designed to provide validity, accuracy, completeness, consistency, and uniformity of data structure. Also included are routines that provide data process/flow validation and correction such as data auditing, workflow specification, workflow execution, and post-processing and controlling.		
Master Data Management:	A platform that allows the MSP to create, maintain and update data models, provide for data on-ramps that manage attributes and values of source data, and the creation of rule-sets for data quality, match/merge processes, and error remediation.		
The MSP Data Hub:	A mapped, indexed, cleansed and modeled data environment that contains live, delayed and static data from multiple repositories, both external and internal to the MSP. The Hub can also map unindexed data to leverage combined analytics from unstructured data.		
Web Focus Law Enforcement Right To Use License (LERTU):	Web Focus is used for the front end of reporting for data within the MSP's Data Hub. The vendor must be able to make use of the MSP's LETRU license of the Web Focus environment for advanced analytics and ad hoc reporting	OR	Be able to embed the Web Focus component into a native interface for analysis, metrics, and ad hoc reporting.

The MSP's Data Hub Environment consists of four major components which are outlined below.			
Law Enforcement Data Model:	The vendor must be able to modify and/or update the MSP's current Law Enforcement Data Model to include adding new elements, and/or legacy data under previously mastered domains which include location, person, activity, vehicle, and weapon, if applicable. New elements must be cleansed, geocoded, mastered, indexed and mapped to the applications, reports and/or systems that leverage them, if applicable. The modification and updating of the MSP Data Model must be done with care not to disrupt current dataflow and application interfaces, in any environment (Development, Test, and Production).	OR	Be willing to sub-contract the work related to the data model to an appropriate group, talent or agency. All submitted pricing must include this additional component.
Integration of Legacy Data:	Integration of legacy data must be completed using native tools within the MSP Data Hub environment. All legacy data must be either stored and/or replicated to the MSP Data Hub. The decision on whether to use the MSP Hub as a storage point for replicated data and/or a primary storage and transactional point will be up to the MSP. All vendors must provide both options, along with associated pricing.		
Interfaces:	All external interfaces must be completed using the MSP Data Access Layer associated with the MSP Hub Environment. External interfaces and/or vendors that are proposing offsite hosting must provide an Application Programming Interface (API) (with associated schema and data dictionaries), Gateway Service (included in the price of hosting), or another acceptable means of direct data transfer to the MSP Hub environment.		
Input Cleansing:	Any forward-facing application must, as much as possible, be able to make real-time calls to the data mastering and cleansing routines within the Hub environment to ensure that data input is as accurate as possible for operational use.		

11. SOFTWARE

Contractor must deliver a Sex Offender Registry (SOR) solution that is configured to MSP's specific needs. Under the "modified off-the-shelf" (MOTS) solution approach the core functionality in our pre-existing technology framework and further develop solution layers to MSP's specifications.

12. SOLUTION REQUIREMENTS
See section **Exhibit A - Table 1 Business Specification Worksheet** for more details on the requirements of this Contract.

13. INTEGRATION
Contractor solution will comply with MSP's integration requirements, per the below chart.

Numbers	Category	Volume of Data	Interface Agency	Tab or Field	Description	Connection Frequency	Priority Level
REQUIRED							
1	Interface	50,000 Records per day (nightly)	Criminal History Record (CHR)	Prints	The System must be able to interface with Criminal History Record (CHR) which Add palm prints, fingerprints, and DNA to SOR record.	MSP is expected to receive and sync all updates through a nightly batch process.	High
Contractor Requirement	Coplogic will build an interface with CHR. In Kentucky, we interface with KSP's CHR through the state message switch (which, like in Michigan, is provided by Computer Projects of Illinois, or CPI). Coplogic has interfaced with CPI message switches and criminal history databases in support of many statewide programs.						
2	Interface	20,000 Records per month (1 time a month)	MI Cashiering and Receiving System (MiCars)	Fees	The System must be able to interface with MI Cashiering and Receiving System (MiCars). Have the ability to send fee information to MiCars for creation of billing/invoicing.	MSP is expecting the data to be sent to the SOR system once a month.	High
Contractor Requirement	Coplogic will build an interface with MiCars to comply with this requirement. We have previously developed similar functionality to send fee information for creation of billing/invoicing. For example, in two Midwestern U.S. states, Coplogic has built statewide electronic systems that allow the public to securely remit payment for firearms licenses through an online portal.						

Numbers	Category	Volume of Data	Interface Agency	Tab or Field	Description	Connection Frequency	Priority Level
3	Interface	50,000 Records per day (real-time)	Law Enforcement Information Network (LEIN)	Warrants	The System must be able to interface with Law Enforcement Information Network (LEIN). when a warrant is entered into LEIN,	Michigan State Police would need the system to automatically update the warrant information in the SOR system once a day.	High
Contractor Requirement	Coplogic will build an interface to LEIN. We anticipate being able to access LEIN through the state message switch (CPI).						
3.1	Interface	50,000 Records per day (real-time)	Law Enforcement Information Network (LEIN)	Vehicles	The Contractor system shall be able to update a status change and populate by entering the license plate number and all available fields in LEIN.	Michigan State Police would need the contractor system to auto-update the vehicle information in the SOR system once day.	Medium
Contractor Requirement	Coplogic will develop this functionality as part of our solution for MSP. We also perform vehicle searches against LINK/NCIC.						
4	Interface	18,000 Records per day (nightly)	Michigan Dept. of Corrections (MDOC)	MDOC Information	System must be able to interface with (MDOC) to capture information such as parole, probation, incarceration, offense. Any information necessary to eliminate need for duplicate entry between MSP SOR and MDOC.	MSP is expected to receive and sync all updates through a nightly batch process.	High

Numbers	Category	Volume of Data	Interface Agency	Tab or Field	Description	Connection Frequency	Priority Level
Contractor Requirement	Coplogic will build an interface to facilitate this feature. Our current SOR has an existing interface to the Kentucky Offender Management System (KOMS) for eWarrants and eCitation applications.						
5	Interface	60,000 Records per day (real-time)	National Sex Offender Public Website (NSOPW)	Website	The System shall be able to interface with MI SOR SYSTEM sending registered sex offender information to NSOPW.	Real Time	High
Contractor Requirement	Coplogic will leverage our current system and capabilities to provide MSP with an option for the upload of offender data to NSOPW in the most current version of NIEM.						
6	Interface	50,000 Records per day (real-time)	Statewide Network Agency Photos (SNAP)	Photos	The System must be able to interface with the Statewide Network Agency Photos (SNAP) application so that when an offender gets new SOS photo or mugshot this should auto change the photo for SOR, date of change and possible expiration of photo (if applicable).	Real Time	High
Contractor Requirement	Coplogic will build an interface to facilitate this feature.						

Numbers	Category	Volume of Data	Interface Agency	Tab or Field	Description	Connection Frequency	Priority Level
7	Interface	50,000 Records per month (1 time a month)	Secretary of State (SOS)	Death	The System shall be able to interface with Secretary of State (SOS) which provides Information regarding death of a registered sex offender.	MSP is expected to receive and sync all updates monthly	Medium
Contractor Requirement	Coplogic will build an interface to facilitate this feature. As our LNRS affiliate already receives State of Michigan death records in connection with other business programs, Coplogic is also willing to explore whether there are any efficiencies that could be realized by leveraging an existing LNRS interface.						
7.1	Interface	50,000 Records per month (1 time a month)	Secretary of State (SOS)	Driver's License/PID	The System shall be able to interface with Secretary of State (SOS) providing issue and expiration dates and license type and state.	MSP is expected to receive and sync all updates monthly	Medium
Contractor Requirement	Coplogic will build an interface to facilitate this feature. In connection with other statewide projects, Coplogic has previously interfaced with state agencies to obtain driver's license information for verification purposes.						
7.2	Interface	50,000 Records per month (1 time a month)	Secretary of State (SOS)	Photos	The System shall be able to interface with Secretary of State (SOS) providing registered sex offender photos as they are updated within MIDIRS.	MSP is expected to receive and sync all updates monthly	Low
Contractor Requirement	Coplogic will build an interface to facilitate this feature.						

Numbers	Category	Volume of Data	Interface Agency	Tab or Field	Description	Connection Frequency	Priority Level
7.3	Interface	50,000 Records per month (1 time a month)	Secretary of State (SOS)	Vehicles	The System shall be able to interface with Secretary of State (SOS). When a register sex offender registers a vehicle, the system should prepopulate the SOR system. Date stamped with a start date.	MSP is expected to receive and sync all updates monthly	Medium
Contractor Requirement	Coplogic will build an interface to facilitate this feature.						
8	Interface	2,600MB per day	Michigan State Police Dashboard	Website	System must be able to interface with MSP Dashboard sending monthly statistical information based on Districts and Posts.	Monthly	High
Contractor Requirement	Coplogic has an interface to facilitate this feature.						
OPTIONAL							

Numbers	Category	Volume of Data	Interface Agency	Tab or Field	Description	Connection Frequency	Priority Level
9	Interface	18,000 Records per day (nightly)	Federal Bureau of Prisons (FBOP)	Address	The System must be able to interface with Federal Bureau of Prisons (FBOP) that identifies when an offender is in federal prison.	Michigan State Police would need the system to automatically update the address and information in the SOR system as status changes with change date	High
Contractor Requirement	Coplogic is able to build an interface to facilitate this feature, upon request from MSP						
10	Interface	1,000 Record per month (1 time a month)	Immigration and Custom Enforcement (I.C.E.)	Address	The Contractor System shall be able to interface with Immigration and Custom Enforcement (I.C.E.) system that identifies when an offender has been deported.	MSP is expected to receive and sync all updates monthly	Medium
Contractor Requirement	Coplogic is able to build an interface to facilitate this feature. In Kentucky, we interface with I.C.E. through the state message switch (which, as in Michigan, is provided by CPI). We understand this is an optional interface, available upon request.						
11	Interface	50,000 Records per month (1 time a month)	Michigan Dept of Health and Human Services - BRIDGES (MDHHS)	Bridge card	Identify offenders who have a bridge card.	Monthly	Medium
Contractor Requirement	Coplogic will build an interface to facilitate this feature, upon request.						

Numbers	Category	Volume of Data	Interface Agency	Tab or Field	Description	Connection Frequency	Priority Level
12	Interface	5,000 Records per month (1 time a month)	Enforcement Automated Criminal Incident System (EAICS)	Statistical - Arrest for SOR Violations	The ability to collect arrests for SOR violations (arrest codes 5089 through 5092). This information is needed for SOR Monthly Summary Report.	Monthly	Low
Contractor Requirement	Coplogic has an interface to facilitate this feature. This effort will be greatly facilitated by Coplogic's status as the vendor that developed eAICS and other field-based reporting tools for MSP. (See **Section G.2**.)						
13	Interface	5,000 Records per month (1 time a month)	State Management Record System (SRMS)	Statistical - Arrest for SOR Violations	The ability to collect arrests for SOR violations (arrest codes 5089 through 5092). This information is needed for SOR Monthly Summary Report.	Monthly	Low
Contractor Requirement	Coplogic will build an interface to facilitate this feature, upon request.						

14. MIGRATION

Current Technology	**MS SQL / Web Services**
Data Format	**Web Services – NIEM XML**
Number of Data Fields	**500+ fields**
Number of Records	**63,815**
Data base current size	**1GB**
Contractor's Requirement	As part of this engagement, Coplogic will execute a data migration plan. Our standard process includes following a data conversion schedule, data conversion specifications, and data conversion plan. The development, implementation, and execution of the conversion

	generally takes place concurrently with the review, development, and implementation of other components of the solution. Coplogic will work with MSP's SOR subject matter experts in the development and testing of data migration scripts and the testing of migrated data. We will dedicate a qualified project team that will leverage experience gained from other statewide project conversions.

15. TESTING SERVICES AND ACCEPTANCE
Contractor accepts **Section 11. Pre-Delivery Testing and Section 12. Acceptance Testing**, **of the COTS Contract Terms**.

16. TRAINING SERVICES
Contractor must develop a full Training Management Plan that encompasses the entire lifecycle of the contract – including implementation, go-live support, the transition to self-sufficiency, and continuing thereafter on an ongoing basis. Contractor will consult MSP in designing this plan, which will note class sizes, materials to be provided, class duration, and other details.

As requirements change with SORNA adoption, contractor will progressively train users on best practices to meet new requirements. The SOR application will have 7,000+ users, all of which will require application training. Contractor must provide available training options that address the need to train all users of the application for initial implementation and throughout the term of the contract. This includes but is not limited to, on-site, "train the trainer", and forms of remote training, such as webinars, and video conferencing.

Contractor must hold instructor-led ("train the trainer") sessions in addition to providing documentation for the SOR solution. Contractor will create, and consistently update a user manual/training guide with a synopsis of standard operating procedures specific to MSP needs. Contractor must provide details on, and examples of, clearly written instructions and documentation to enable State administrators and end-users to successfully operate the Solution without needing to bring in additional Contractor support.

17. HOSTING
Externally Hosted
An externally hosted solution using a FedRAMP-compliant third-party cloud service provider, such as Microsoft Azure or Amazon Web Services (AWS).

Contractor must maintain and operate a backup and disaster recovery plan to achieve a Recovery Point Objective (RPO) of 4 hours, and a Recovery Time Objective (RTO) of 4 hours.

18. SUPPORT AND OPERATIONS
The State requires the Contractor to provide second line support during the hours of 8 a.m. to 5 p.m. Eastern, Monday thru Friday, excluding government identified holidays.

Tier Definition	Responsibility
Tier 1 refers to basic help desk support (such as resetting passwords).	MSP
Tier 2 refers to more in-depth technical support. Problems that are not able to be resolved through the Tier 1 help desk will be sent to Tier 2.	Coplogic

Tier Definition	Responsibility
Tier 3 refers to support provided by expert-level system support and development staff members.	Coplogic
Tier 4 refers to support that must be escalated and requires coding changes to the application.	Coplogic

a) Help desk support is available 8 a.m. to 5 p.m. Eastern, Monday thru Friday, excluding government identified holidays.
b) Contractor to provide a Web-enabled help desk interface should be provided to assist with communication between the vendor and MSP. This will provide for interactive communication and on-going tracking of progress for any issue; available for the SOR Unit staff or other authorized/designated MSP employees, at no additional cost.
c) Calls for service must be answered by the next business day.

19. DOCUMENTATION

Contractor must provide all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

Contractor must develop and submit for State approval complete, accurate, and timely Solution documentation to support all users, and will update any discrepancies, or errors through the life of the contract.

The Contractor's user documentation must provide detailed information about all software features and functionality, enabling the State to resolve common questions and issues prior to initiating formal support requests.

20. TRANSITION SERVICES

Upon termination or expiration of the agreement, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the agreement to continue without interruption or adverse effect, and to facilitate the orderly transfer of the services to the State or its designees. Such transition assistance may include but is not limited to: (a) continuing to perform the services at the established rates; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable services to the State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return (in a format specified by the State) to the State all data stored in the solution; and (d) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts.

21. PRODUCTS AND SERVICES

Reserved.

22. CONTRACTOR KEY PERSONNEL

Contractor Contract Administrator. Must identify the individual appointed by it to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

Contractor
Name: Mary Roush **Address: Lansing, MI** **Phone: 517-881-4142** **Email: Mary.Roush@lexisnexisrisk.com**

Contractor Project Manager. Must identify the Contractor Project Manager who will serve as the primary contact with regard to services who will have the authority to act on behalf of the Contractor in matters pertaining to the implementation services.

Contractor
Name: Chris Sowerwine **Address: Remote** **Phone: 608-819-5305** **Email: Christopher.sowerwine@lexisnexisrisk.com**

Contractor Service Manager. Contractor to provide name of individual to serve as primary contact with respect to the Services, who will have the authority to act on behalf of Contractor in matters pertaining to the receipt and processing of Support Requests and the Support Services.

Contractor
Name: Mary Roush **Address: Lansing, MI** **Phone: 517-881-4142** **Email: Mary.Roush@lexisnexisrisk.com**

Contractor Security Officer. Contractor to provide name of individual to respond to State inquiries regarding the security of the Contractor's systems. This person must have sufficient knowledge of the security of the Contractor Systems and the authority to act on behalf of Contractor in matters pertaining thereto.

Contractor
Name: Flavio Villanustre **Address: Remote** **Phone: 770-752-3320** **Email: Flavio.villanustre@lexisnexisrisk.com**

23. CONTRACTOR PERSONNEL REQUIREMENTS

Contractor must present evidence, satisfactory to MSP, of Michigan State Police Background checks and drug tests for all staff identified for assignment to this project; and is to include subcontracted staff.

Prior to assignment the contractor will complete a state and federal fingerprint background for all personnel, including subcontracted personnel, who have direct access to State's data and for those who have direct responsibility to configure and maintain computers system and networks with direct access to State's data.

a) For a Michigan resident, Contractor personnel will complete and sign a CJIS-008 form and submit to Live Scan fingerprinting with an authorized vendor.
b) For non-Michigan residents, Contractor personnel and subcontracted personnel will be required to complete and submit a RI-008 Fingerprint Card for the National Crime Information Center (NCIC) Finger Prints and a CJIS-008 Background Authorization Request form.

Contractor will pay for all costs associated with ensuring their staff meets all requirements.

24. STATE RESOURCES/RESPONSIBILITIES

The State will provide the following resources as part of the implementation and ongoing support of the Solution.

State Contract Administrator. The State Contract Administrator is the individual appointed by the State to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

State Project Manager. The State Project Manager will serve as the primary contact with regard to implementation Services who will have the authority to act on behalf of the State in approving Deliverables, and day to day activities.

Agency Business Owner. The Agency Business Owner will serve as the primary contact for the business area with regard to business advisement who will have the authority to act on behalf of the State in matters pertaining to the business Specifications.

State Technical Lead. The State Technical Lead will serve as the primary contact with regard to implementation technical advisement.

25. MEETINGS

At start of the engagement, the Contractor Project Manager must facilitate a project kick off meeting with the support from the State's Project Manager and the identified State resources to review the approach to accomplishing the project, schedule tasks and identify related timing, and identify any risks or issues related to the planned approach. From project kick-off until final acceptance and go-live Contractor, at no cost to the state, is to plan quarterly in person on-site meetings to facilitate project progress. Additionally, Contractor Project Manager must facilitate weekly meetings (or more if determined necessary by the parties) to provide updates on implementation progress. Following go-live, Contractor must facilitate monthly meetings (or more or less if determined necessary by the parties) to ensure ongoing support success. Meetings may be by phone, Skype, teleconference, or other agreeable means of communication.

26. PROJECT REPORTS

Once the Project Kick-Off meeting has occurred, the Contractor Project Manager will monitor project implementation progress and report on a weekly basis to the State's Project Manager the following:

- Progress to complete milestones, comparing forecasted completion dates to planned and actual completion dates
- Accomplishments during the reporting period
- Tasks planned for the next reporting period
- Identify any existing issues which are impacting the project and the steps being taken to address those issues
- Identify any new risks and describe progress in mitigating high impact/high probability risks previously identified

27. MILESTONES AND DELIVERABLES

The State's proposed milestone schedule and associated deliverables are set forth below.

Milestone Event	**Associated Milestone Deliverable(s)**	**Schedule** (calendar days)
Team Building / Ramp up	Project Kickoff	Contract Execution + 60 days
Project Planning	Project Kickoff	Contract Execution + 70 days (10 days)

Requirements and Design Validation	Validation sessions, Final Requirement Validation Document, Final Design Document, Final Implementation Document	Execution + 130 days (60 days)
Provision environments	Validate Test and Production environments	Execution + 130 days (60 days parallel to req gathering)
Installation, Integration, Migration and Configuration of software	Final Solution and Testing Document	Execution + 370 days (240 days)
Testing and Acceptance	Final Test Results Report, Final Training Documentation, Final Acceptance	Execution + 400 days (30 days)
Post-Production Warranty	Maintenance and Support (free of charge)	Production + 90 days
Production Support Services	Ongoing after Final Acceptance.	Ongoing

The Contractor Project Manager will be responsible for maintaining an MS Project schedule (or approved alternative) identifying tasks, durations, forecasted dates and resources – both Contractor and State - required to meet the timeframes as agreed to by both parties.

Changes to scope, schedule or cost must be addressed through a formal change request process with the State and the Contractor to ensure understanding, agreement and approval of authorized parties to the change and clearly identify the impact to the overall project.

SUITE Documentation
In managing its obligation to meet the above milestones and deliverables, the Contractor is required to utilize the applicable State Unified Information Technology Environment (SUITE) methodologies, or an equivalent methodology proposed by the Contractor.

SUITE's primary goal is the delivery of on-time, on-budget, quality systems that meet customer expectations. SUITE is based on industry best practices, including those identified in the Project Management Institute's PMBoK and the Capability Maturity Model Integration for Development. It was designed and implemented to standardize methodologies, processes, procedures, training, and tools for project management and systems development lifecycle management. It offers guidance for efficient, effective improvement across multiple process disciplines in the organization, improvements to best practices incorporated from earlier models, and a common, integrated vision of improvement for all project and system related elements.

While applying the SUITE framework through its methodologies is required, SUITE was not designed to add layers of complexity to project execution. There should be no additional costs from the Contractor, since it is expected that they are already following industry best practices which are at least similar to those that form SUITE's foundation.

SUITE's companion templates are used to document project progress or deliverables. In some cases, the Contractor may have in place their own set of templates for similar use. Because SUITE can be tailored to fit specific projects, project teams and State project managers may decide to use the Contractor's provided templates, as long as they demonstrate fulfillment of the SUITE methodologies.

The Contractor is required to review http://www.michigan.gov/suite and demonstrate how each PMM/SEM requirement will be met. Contractors wishing to use their own documents must submit an example of the document that will be substituted. If the Contractor deems a document to be non-applicable, please provide reasons for the determination. The State reserves the right to give final approval of substituted documents and items marked as non-applicable.

28. PRICING

If Contractor reduces its prices for any of the software or services during the term of this Contract, the State shall have the immediate benefit of such lower prices for new purchases. Contractor shall send notice to the State's Contract Administrator with the reduced prices within fifteen (15) Business Days of the reduction taking effect.

Travel and Expenses

The State does not pay for overtime or travel expenses.

29. ADDITONAL INFORMATION

The State reserves the right to purchase any additional services or products from the Contractor during the duration of the Contract.

Schedule C - Licensing Agreement

1. Grant of Rights and License Restrictions.

a. Right to Use. Contractor hereby grants to the State, for the Term of this Agreement, a limited, non-exclusive, perpetual, non-assignable, non-sublicensable, and non-transferable right to use Contractor's Software, the related database, and related hardware and other infrastructure (the "Sex Offender Registry (SOR) System") for an unlimited number of Users within the State [to be defined to include users from agencies within State – DA, PD, Probation, local PDs, CHP, etc.] to this Schedule C (Licensing Agreement).

b. Use Restrictions. The Software shall only be used by the State and an unlimited number of User within the State [to be defined to include users from agencies within State – DA, PD, Probation, local PDs, CHP, etc.] to this Schedule C (Software License Appendix). State shall prevent access to the Sex Offender Registry System by unauthorized users and immediately notify Contractor of suspected or known unauthorized use. The State shall not, and shall not permit any third-party to: (i) reverse engineer, decompile, or disassemble the Software; (ii) attempt in any other manner to obtain the source code; (iii) create copies, or derivative works of, reconfigure or modify the Software, or Documentation; (iv) resell, rent, lease, or transfer the Software or otherwise make it available to other parties not authorized to use the Software, (v) use the Software for marketing or commercial solicitation purposes, resell, or broker the Software to any third-party or otherwise use the Software for any personal (non-law enforcement) purposes, (vi) access or use the Software from outside the United States without Contractor's prior written approval, (vii) use the Software to create a competing product or provide data processing services to third parties; (viii) harvest, post, transmit, copy, modify, create derivative works from, tamper, distribute the Software, or in any way circumvent the navigational structure of the Software, including to knowingly upload or transmit any computer viruses, Trojan Horses, worms or anything else designed to interfere with, interrupt or disrupt the normal operating procedures of Software; (ix) use the Software to store or transmit infringing, libelous, or otherwise unlawful or tortuous material, or to store or transmit material in violation of third-party privacy rights or otherwise infringe on the rights of others; (x) reveal any user accounts or passwords for the Software to any third parties (third parties shall not include State employees or subcontractors or other Users identified in Schedule C, who have a need to know such information); and. State further agrees that it shall comply with all laws, regulations, and rules which govern the use of the Software.

c. End-User License Agreement. The State acknowledges and agrees that any end-user license terms and conditions governing the use of the Software by the public shall be determined by the State; provided however that such terms and conditions are no less restrictive than those set forth in this Schedule C.

Schedule E - Service Level Agreement

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Section 1** shall have the respective meanings given to them in the Contract.

"**Actual Uptime**" means the total minutes in the Service Period that the Hosted Services are Available.

"**Availability**" has the meaning set forth in **Section 4.1**.

"**Availability Requirement**" has the meaning set forth in **Section 4.1**.

"**Available**" has the meaning set forth in **Section 4.1**.

"**Contractor Service Manager**" has the meaning set forth in **Section 3.1**.

"**Corrective Action Plan**" has the meaning set forth in **Section 5.6**.

"**Critical Service Error**" has the meaning set forth in **Section 5.4(a)**.

"**Exceptions**" has the meaning set forth in **Section 4.2**.

"**Force Majeure Event**" has the meaning set forth in **Section 6.1**.

"**High Service Error**" has the meaning set forth in **Section 5.4(a)**.

"**Hosted Services**" has the meaning set forth in **Section 2.1(a)**.

"**Low Service Error**" has the meaning set forth in **Section 5.4(a)**.

"**Medium Service Error**" has the meaning set forth in **Section 5.4(a)**.

"**Resolve**" has the meaning set forth in **Section 5.4(b)**.

"**Scheduled Downtime**" has the meaning set forth in **Section 4.3**.

"**Scheduled Uptime**" means the total minutes in the Service Period.

"**Service Availability Credits**" has the meaning set forth in **Section 4.6(a)**.

"**Service Error**" means any failure of any Hosted Service to be Available or otherwise perform in accordance with this Schedule.

"**Service Level Credits**" has the meaning set forth in **Section 5.5**.

"**Service Level Failure**" means a failure to perform the Software Support Services fully in compliance with the Support Service Level Requirements.

"**Service Period**" has the meaning set forth in **Section 4.1**.

"**Software**" has the meaning set forth in the Contract.

"**Software Support Services**" has the meaning set forth in **Section 5**.

"**State Service Manager**" has the meaning set forth in **Section 3.2**.

"**State Systems**" means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the State or any of its designees.

"**Support Request**" has the meaning set forth in **Section 5.4(a)**.

"**Support Service Level Requirements**" has the meaning set forth in **Section 5.4**.

"**Term**" has the meaning set forth in the Contract.

2. Services.

2.1. Services. Throughout the Term, Contractor will, in accordance with all terms and conditions set forth in the Contract and this Schedule, provide to the State and its Authorized Users the following services:

(a) the hosting, management and operation of the Software and other services for remote electronic access and use by the State and its Authorized Users ("**Hosted Services**");

(b) the Software Support Services set forth in **Section 5** of this Schedule;

3. Personnel

3.1. Contractor Personnel for the Hosted Services. Contractor will appoint a Contractor employee to serve as a primary contact with respect to the Services who will have the authority to act on behalf of Contractor in matters pertaining to the receipt and processing of Support Requests and the Software Support Services (the "**Contractor Service Manager**"). The Contractor Service Manager will be considered Key Personnel under the Contract.

3.2. State Service Manager for the Hosted Services. The State will appoint and, in its reasonable discretion, replace, a State employee to serve as the primary contact with respect to the Services who will have the authority to act on behalf of the State in matters pertaining to the Software Support Services, including the submission and processing of Support Requests (the "**State Service Manager**").

4. Service Availability and Service Availability Credits.

4.1. Availability Requirement. Contractor will make the Hosted Services Available, as measured over the course of each calendar month during the Term and any additional periods during which Contractor does or is required to perform any Hosted Services (each such calendar month, a "**Service Period**"), at least 99.9% of the time, excluding only the time the Hosted Services are not Available solely as a result of one or more Exceptions (the "**Availability Requirement**"). "**Available**" means the Hosted Services are available and operable for access and use by the State and its Authorized Users over the Internet in material conformity with the Contract. "**Availability**" has a correlative meaning. The Hosted Services are not considered Available in the event of a material performance degradation or inoperability of the Hosted Services, in whole or in part. The Availability

Requirement will be calculated for the Service Period as follows: (Actual Uptime – Total Minutes in Service Period Hosted Services are not Available Due to an Exception) ÷ (Scheduled Uptime – Total Minutes in Service Period Hosted Services are not Available Due to an Exception) x 100 = Availability.

4.2. Exceptions. No period of Hosted Service degradation or inoperability will be included in calculating Availability to the extent that such downtime or degradation is due to any of the following ("**Exceptions**"):

(a) failures of the State's or its Authorized Users' internet connectivity;

(b) Scheduled Downtime as set forth in **Section 4.3**.

4.3. Scheduled Downtime. Contractor must notify the State at least five (5) days in advance of all scheduled outages of the Hosted Services in whole or in part ("**Scheduled Downtime**"). All such scheduled outages will: (a) last no longer than five (5) hours; (b) be scheduled between the hours of 12:00 a.m. and 5:00 a.m., Eastern Time; and (c) occur no more frequently than once per week; provided that Contractor may request the State to approve extensions of Scheduled Downtime above five (5) hours, and such approval by the State may not be unreasonably withheld or delayed.

4.4. Software Response Time. Software response time, defined as the interval from the time the end user sends a transaction to the time a visual confirmation of transaction completion is received, must be less than or equal to two (2) seconds for 98% of all transactions. Software Response Time will be measured from the time that the Coplogic web server receives the request.

4.5. Service Availability Reports. Within thirty (30) days after the end of each Service Period, Contractor will provide to the State a report describing the Availability and other performance of the Hosted Services during that calendar month as compared to the Availability Requirement. The report must be in electronic or such other form as the State may approve in writing and shall include, at a minimum: (a) the actual performance of the Hosted Services relative to the Availability Requirement; and (b) if Hosted Service performance has failed in any respect to meet or exceed the Availability Requirement during the reporting period, a description in sufficient detail to inform the State of the cause of such failure and the corrective actions the Contractor has taken and will take to ensure that the Availability Requirement are fully met.

4.6. Remedies for Service Availability Failures.

(a) If the actual Availability of the Hosted Services is less than the Availability Requirement for any Service Period, such failure will constitute a Service Error for which Contractor will issue to the State the following credits on the fees payable for Hosted Services provided during the Service Period ("**Service Availability Credits**"):

Availability	Credit of Fees
≥99.9%	None
<99.9% but ≥99.0%	7.5%
<99.0% but ≥95.0%	25%
<95.0%	50%

(b) Any Service Availability Credits due under this **Section 4.6** will be applied in accordance with payment terms of the Contract.

(c) If the actual Availability of the Hosted Services is less than the Availability Requirement in any two (2) of four (4) consecutive Service Periods, then, in addition to all other remedies available to the State, the State may terminate the Contract on written notice to Contractor with no liability, obligation or penalty to the State by reason of such termination.

5. Support and Maintenance Services. Contractor will provide Hosted Service maintenance and support services (collectively, "**Software Support Services**") in accordance with the provisions of this **Section 5**. The Software Support Services are included in the Services, and Contractor may not assess any additional fees, costs or charges for such Software Support Services.

5.1. Support Service Responsibilities. Contractor will:

(a) correct all Service Errors in accordance with the Support Service Level Requirements, including by providing defect repair, programming corrections and remedial programming;

(b) provide unlimited telephone support 8 a.m. to 5 p.m. Eastern, Monday thru Friday,

(c) provide unlimited online support 24 hours a day, seven days a week;

(d) provide online access to technical support bulletins and other user support information and forums, to the full extent Contractor makes such resources available to its other customers; and

(e) respond to and Resolve Support Requests as specified in this **Section 5**.

5.2. Service Monitoring and Management. Contractor will continuously monitor and manage the Hosted Services to optimize Availability that meets or exceeds the Availability Requirement. Such monitoring and management includes:

(a) proactively monitoring on a twenty-four (24) hour by seven (7) day basis all Hosted Service functions, servers, firewall and other components of Hosted Service security;

(b) if such monitoring identifies, or Contractor otherwise becomes aware of, any circumstance that is reasonably likely to threaten the Availability of the Hosted Service, taking all necessary and reasonable remedial measures to promptly eliminate such threat and ensure full Availability; and

(c) if Contractor receives knowledge that the Hosted Service or any Hosted Service function or component is not Available (including by written notice from the State pursuant to the procedures set forth herein):

(i) confirming (or disconfirming) the outage by a direct check of the associated facility or facilities;

(ii) if Contractor's facility check in accordance with clause (i) above confirms a Hosted Service outage in whole or in part: (A) notifying the State in writing pursuant to the procedures set forth herein that an outage has occurred, providing such details as may be available, including a Contractor trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Section 5.4**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and

(iii) notifying the State that Contractor has fully corrected the outage and any related problems, along with any pertinent findings or action taken to close the trouble ticket.

5.3. Service Maintenance. Contractor will continuously maintain the Hosted Services to optimize Availability that meets or exceeds the Availability Requirement. Such maintenance services include providing to the State and its Authorized Users:

(a) all updates, bug fixes, enhancements, Maintenance Releases, New Versions and other improvements to the Hosted Services, including the Software, that Contractor provides at no additional charge to its other similarly situated customers; provided that Contractor shall consult with the State and is required to receive State approval prior to modifying or upgrading Hosted Services, including Maintenance Releases and New Versions of Software; and

(b) all such services and repairs as are required to maintain the Hosted Services or are ancillary, necessary or otherwise related to the State's or its Authorized Users' access to or use of the Hosted Services, so that the Hosted Services operate properly in accordance with the Contract and this Schedule.

5.4. Support Service Level Requirements. Contractor will correct all Service Errors and respond to and Resolve all Support Requests in accordance with the required times and other terms and conditions set forth in this **Section 5.4** ("**Support Service Level Requirements**"), and the Contract.

(a) Support Requests. The State will classify its requests for Service Error corrections in accordance with the descriptions set forth in the chart below (each a "**Support Request**"). The State Service Manager will notify Contractor of Support Requests by email, telephone or such other means as the parties may hereafter agree to in writing.

Support Request Classification	Description: Any Service Error Comprising or Causing any of the Following Events or Effects
Critical Service Error	• Issue affecting entire system or single critical production function; • System down or operating in materially degraded state; • Data integrity at risk; • Declared a Critical Support Request by the State; or • Widespread access interruptions.
High Service Error	• Primary component failure that materially impairs its performance; or • Data entry or access is materially impaired on a limited basis.
Medium Service Error	• Hosted Service is operating with minor issues that can be addressed with an acceptable (as determined by the State) temporary work around.
Low Service Error	• Request for assistance, information, or services that are routine in nature.

(b) Response and Resolution Time Service Levels. Response and Resolution times will be measured from the time Contractor receives a Support Request until the respective times Contractor has (i) responded to, in the case of response time and (ii) Resolved such Support Request, in the case of Resolution time. "**Resolve**" (including "**Resolved**", "**Resolution**" and correlative capitalized terms) means that, as to any Service Error, Contractor has provided the State the corresponding Service Error correction and the State has confirmed such correction and its acceptance thereof. Contractor will respond to and Resolve all Service Errors within the following times based on the severity of the Service Error:

(c) Escalation. With respect to any Critical Service Error Support Request, until such Support Request is Resolved, Contractor will escalate that Support Request within sixty (60) minutes of the receipt of such Support Request by the appropriate Contractor support personnel, including, as applicable, the Contractor Service Manager and Contractor's management or engineering personnel, as appropriate.

5.5. Support Service Level Credits. Failure to achieve any of the Support Service Level Requirements for Critical and High Service Errors will constitute a Service Level Failure for which Contractor will issue to the State the corresponding service credits set forth in **Section 5.4(b)** ("**Service Level Credits**") in accordance with payment terms set forth in the Contract.

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
Critical Service Error	2 hours. The State shall submit a Support Request by telephone using the Point of Contact Escalation chart provided. Once the State has spoken to one of the Contacts listed, the State shall submit a follow up email to Contractor, and Contractor shall acknowledge receipt of the Support Request via email to the State within two (2) hours of receipt of the email as provided above.	8 hours Contractor shall resolve the Support Request as practicable and no later than eight (8) hours after Contractor's receipt of the Support Request. If the State and Contractor agree to resolve the Support Request by way of a work-around, the severity level assessment will be reduced to a Severity Level of Error 2, until a permanent solution is agreed upon by both parties. This "work-around" will be agreed upon by both parties in writing prior to implementation.	2.5% of the Fees for the month in which the initial Service Level Failure begins and two point five percent (2.5%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time. This credit will be translated to hours that can be applied to future modifications of any system or application developed by the contractor and built for use or licensed by MSP-CJIC or designee.	2.5% of the Fees for the month in which the initial Service Level Failure begins and two point five percent (2.5%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment. This credit will be translated to hours that can be applied to future modifications of any system or application developed by the contractor and built for use or licensed by MSP-CJIC or designee.

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
		The Contractor will provide any training updates on end user functionality, due to the "work-around" to the State.	These hours will be calculated at $115 per hour. The credit translated to hours, for an individual incident, will be capped at 7% of the total maintenance fee. Subsequent incidents will be cumulative but the total number of hours translated will be capped at 20% of the total maintenance fees for the Sex Offender Registry application. Agreement to apply provision requires agreement of both the vendor and the State.	These hours will be calculated at $115 per hour. The credit translated to hours, for an individual incident, will be capped at 7% of the total maintenance fee. Subsequent incidents will be cumulative but the total number of hours translated will be capped at 20% of the total maintenance fees for the Sex Offender Registry application. Agreement to apply provision requires agreement of both the vendor and the State.

High Service Error	1 day The State shall submit a Support Request by telephone using the Point of Contact Escalation chart provided. Once the State has spoken to one of the Contacts listed, the State shall submit a follow up email to Contractor, and Contractor shall acknowledge receipt of the support request via email to the State. Contractor will provide: a. The State receipt of the acceptance of a "Critical Service Error" work-around, within twenty-four (24) hours of receipt of the email from the State as provided above, which allows the State to confirm that they have accepted a work around. b. The State with confirmation of receipt of a "High Service Error" level support request within twenty-four	2 days Contractor shall resolve the Support Request as soon as practicable and no later than two (2) Business Days after the State's written acceptance of a "Critical Service Error" work-around or the Contractor's receipt of the Support Request, where applicable.	1% of the Fees for the month in which the initial Service Level Failure begins and three percent (1%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time. This credit will be translated to hours that can be applied to future modifications of any system or application developed by the contractor and built for use or licensed by MSP-CJIC or designee. These hours will be calculated at $115 per hour. The credit translated to hours, for an individual incident, will be capped at 7% of the total maintenance fee. Subsequent incidents will be cumulative but the	1% of the Fees for the month in which the initial Service Level Failure begins and three percent (1%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment. This credit will be translated to hours that can be applied to future modifications of any system or application developed by the contractor and built for use or licensed by MSP-CJIC or designee. These hours will be calculated at $115 per hour. The credit translated to hours, for an individual incident, will be capped at 7% of the total maintenance fee.

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
	(24) hours from the time Contractor receives the email from the State as provide above.		total number of hours translated will be capped at 20% of the total maintenance fees for the Sex Offender Registry application. Agreement to apply provision requires agreement of both the vendor and the State.	Subsequent incidents will be cumulative but the total number of hours translated will be capped at 20% of the total maintenance fees for the Sex Offender Registry application. Agreement to apply provision requires agreement of both the vendor and the State.
Medium Service Error	3 hours	2 Business Days	N/A	N/A
Low Service Error	2 days	3 weeks +	N/A	N/A

5.6. Corrective Action Plan. If two or more Critical Service Errors occur in any thirty (30) day period during (a) the Term or (b) any additional periods during which Contractor does or is required to perform any Hosted Services, Contractor will promptly investigate the root causes of these Service Errors and provide to the State within five (5) Business Days of its receipt of notice of the second such Support Request an analysis of such root causes and a proposed written corrective action plan for the State's review, comment and approval, which, subject to and upon the State's written approval, shall be a part of, and by this reference is incorporated in, the Contract as the parties' corrective action plan (the "**Corrective Action Plan**"). The Corrective Action Plan must include, at a minimum: (a) Contractor's commitment to the State to devote the appropriate time, skilled personnel, systems support and equipment and other resources necessary to Resolve and prevent any further

occurrences of the Service Errors giving rise to such Support Requests; (b) a strategy for developing any programming, software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of, such Service Errors; and (c) time frames for implementing the Corrective Action Plan. There will be no additional charge for Contractor's preparation or implementation of the Corrective Action Plan in the time frames and manner set forth therein.

6. Force Majeure.

6.1. Force Majeure Events. Subject to **Section 6.3**, neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached the Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of the Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure Event**"), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

6.2. State Performance; Termination. In the event of a Force Majeure Event affecting Contractor's performance under the Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate the Contract by written notice to Contractor if a Force Majeure Event affecting Contractor's performance hereunder continues substantially uninterrupted for a period of five (5) Business Days or more. Unless the State terminates the Contract pursuant to the preceding sentence, any date specifically designated for Contractor's performance under the Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

6.3. Exclusions; Non-suspended Obligations. Notwithstanding the foregoing or any other provisions of the Contract or this Schedule:

(a) in no event will any of the following be considered a Force Majeure Event:

(i) shutdowns, disruptions or malfunctions of Contractor Systems or any of Contractor's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to the Contractor Systems; or

(ii) the delay or failure of any Contractor Personnel to perform any obligation of Contractor hereunder unless such delay or failure to perform is itself by reason of a Force Majeure Event.

(b) no Force Majeure Event modifies or excuses Contractor's obligations under **Sections 19** (State Data), **20** (Confidentiality), or **27** (Indemnification) of the Contract, **Section 7** (Disaster Recovery and Backup) of this Schedule, the Availability Requirement defined in this Schedule, or any security requirements under the Contract, the Statement of Work, or applicable Schedule.

7. Disaster Recovery and Backup. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will:

(a) maintain and operate a backup and disaster recovery plan to achieve a Recovery Point Objective (RPO) of 4 hours, and a Recovery Time Objective (RTO) of 4 hours (the "**DR Plan**"), and implement such DR Plan in the event of any unplanned interruption of the Hosted Services. Contractor's current DR Plan, revision history, and any reports or summaries relating to past testing of or pursuant to the DR Plan are attached as **Schedule G**. Contractor will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance. Contractor will provide the State with copies of all such updates to the Plan within fifteen (15) days of its adoption by Contractor. All updates to the DR Plan are subject to the requirements of this **Section 7**; and

(b) provide the State with copies of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor's receipt or preparation. If Contractor fails to reinstate all material Hosted Services within the periods of time set forth in the DR Plan, the State may, in addition to any other remedies available under this Contract, in its sole discretion, immediately terminate this Contract as a non-curable default.

Schedule F - Data Security Requirements

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Section 1** shall have the respective meanings given to them in the Contract.

"**Contractor Security Officer**" has the meaning set forth in **Section 2** of this Schedule.

"**Contractor Systems**" has the meaning set forth in **Section 5** of this Schedule.

"**FedRAMP**" means the Federal Risk and Authorization Management Program, which is a federally approved risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

"**FISMA**" means The Federal Information Security Management Act 2014 (Pub.L. No. 113-283 (Dec. 18, 2014.)..

"**Hosted Services**" means the hosting, management and operation of the computing hardware, ancillary equipment, Software, firmware, data, other services (including support services), and related resources for remote electronic access and use by the State and its Authorized Users, including any services and facilities related to disaster recovery obligations.

"**NIST**" means the National Institute of Standards and Technology.

"**PSP**" means the State's IT Policies, Standards and Procedures

"**PCI**" means the Payment Card Industry.

2. Contractor will appoint a Contractor employee to respond to the State's inquiries regarding the security of the Contractor Systems who has sufficient knowledge of the security of the Contractor Systems and the authority to act on behalf of Contractor in matters pertaining thereto ("**Contractor Security Officer**"). The Contractor Security Officer will be considered Key Personnel under the Contract.

3. Protection of the State's Confidential Information. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will adhere to the most current version of the FBI CJIS Security Policy, including, but not limited to, the "Shall Statements", the Michigan Addendum and:

3.1. maintain FedRAMP authorization for the Hosted Services throughout the Term, and in the event the contractor is unable to maintain FedRAMP authorization, the State may move the Software to an alternative provider, at contractor's sole cost and expense;

3.2. ensure that the Software and data is securely hosted, supported, administered, and accessed in a data center that resides in the continental United States, and minimally meets Uptime Institute Tier 3 standards (www.uptimeinstitute.com), or its equivalent;

3.3. maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State's Confidential Information that comply with the requirements of the State's data security policies as set forth in the

Contract**,** and must, at a minimum, remain compliant with FISMA and the NIST Special Publication 800.53 (most recent version) MOD Controls using minimum control values as established in the applicable SOM PSP's;

3.4. provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of the State's Confidential Information and the nature of such Confidential Information, consistent with best industry practice and standards;

3.5. take all reasonable measures to:

(a) secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services against "hackers" and others who may seek, without authorization, to disrupt, damage, modify, access or otherwise use Contractor Systems or the information found therein; and

(b) prevent (i) the State and its Authorized Users from having access to the data of other customers or such other customer's users of the Services; (ii) the State's Confidential Information from being commingled with or contaminated by the data of other customers or their users of the Services; and (iii) unauthorized access to any of the State's Confidential Information;

3.6. When data is at rest outside the boundary of a deemed physically secure location, the data shall be encrypted. The cryptographic module used shall be FIPS PUB 140-2 certified and use a symmetric cipher key strength length of at least 256-bits

3.7. When data is transmitted outside the boundary of a deemed physically secure location, the data shall be encrypted. The cryptographic module used shall be FIPS PUB 140-2 certified and use a symmetric cipher key length of at least 128-bits

3.8. In the instances of a physical or digital incident that has a confirmed impact to the security or integrity of State's data, the Contractor will complete and submit a Security Incident Reporting form CJIS-016 to the Michigan State Policy Information Security Officer.

3.9. ensure the Hosted Services support Identity Federation/Single Sign-on (SSO) capabilities using Security Assertion Markup Language (SAML) or comparable mechanisms;

3.10. ensure the Hosted Services have FIPS/NIST compliant multi-factor authentication for privileged/administrative and other identified access; and

3.11. assist the State, at no additional cost, with development and completion of a system security plan using the State's automated governance, risk and compliance (GRC) platform. On an annual basis or as required, re-assessment of the systems controls will be required to receive and maintain authority to operate (ATO). For all findings associated with the Contractor's solution, at no additional cost, identified risks from the SSP will be remediated thru a Plan of Action and Milestones (POAM) process with remediation time frames based on risk level of findings. Contractor will be required to create or assist with the creation of State approved POAMs and perform related remediation activities. The State will make any decisions on Acceptable Risk, the vendor may request risk acceptance, supported by compensating controls, however only the State may formally accept risk.

4. Unauthorized Access. Contractor may not access, and shall not permit any access to, State systems, in whole or in part, whether through Contractor's Systems or otherwise, without the State's express prior written authorization. Such authorization may be revoked by the State in writing at any time in its sole discretion. Any access to State systems must be solely in accordance with the Contract and this Schedule, and in no case exceed the scope of the State's authorization pursuant to this **Section 4**. All State-authorized connectivity or attempted connectivity to State systems shall be only through the State's security gateways and firewalls and in compliance with the State's security policies set forth in the Contract as the same may be supplemented or amended by the State and provided to Contractor from time to time.

5. Contractor Systems. Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems) and networks used by or for Contractor in connection with the Services ("**Contractor Systems**") and shall prevent unauthorized access to State systems through the Contractor Systems.

6. Security Audits. During the Term, Contractor will:

6.1. maintain complete and accurate records relating to its data protection practices, IT security controls, and the security logs of any of the State's Confidential Information, including any backup, disaster recovery or other policies, practices or procedures relating to the State's Confidential Information and any other information relevant to its compliance with this Schedule;

6.2. upon the State's request, make all such records, appropriate personnel and relevant materials available during normal business hours for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) gives Contractor at least five (5) Business Days prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; and (iii) conducts or causes to be conducted such audit in a manner designed to minimize disruption of Contractor's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of the Contract. The State may, but is not obligated to, perform such security audits, which shall, at the State's option and request, include penetration and security tests, of any and all Contractor Systems and their housing facilities and operating environments; and

6.3. if requested by the State, provide a copy of Contractor's FedRAMP System Security Plan within thirty (30) days to the State. The System Security Plan will be recognized as Contractor's Confidential Information.

7. Nonexclusive Remedy for Security Breach. Any failure of the Services to meet the requirements of this Schedule with respect to the security of any State Data or other Confidential Information of the State, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of the Contract for which the State, at its option, may terminate the Contract immediately upon written notice to Contractor without any notice or cure period, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

8. PCI Compliance.

8.1. Contractors that process, transmit, store or affect the security of credit/debit cardholder data, must adhere to the PCI Data Security Standard. The Contractor is responsible for the security of cardholder data in its possession. The data may only be used to assist the State or for other uses specifically authorized by law.

8.2. The Contractor must notify the State's Contract Administrator (within 48 hours of discovery) of any breaches in security where cardholder data has been compromised. In that event, the Contractor must provide full cooperation to the card associations (e.g. Visa, MasterCard, and Discover) and state acquirer representative(s), or a PCI approved third party, to conduct a thorough security review. The Contractor must provide, at the request of the State, the results of such third party security review. The review must validate compliance with the PCI Data Security Standard for protecting cardholder data. At the State's sole discretion, the State may perform its own security review, either by itself or through a PCI approved third party.

8.3. The Contractor is responsible for all costs incurred as the result of the breach. Costs may include, but are not limited to, fines/fees for non-compliance, card reissuance, credit monitoring, and any costs associated with a card association, PCI approved third party, or State initiated security review.

8.4. Without limiting Contractor's obligations of indemnification as further described in this Contract, Contractor must indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the breach.

8.5. The Contractor must dispose of cardholder data when it is no longer needed in compliance with PCI DSS policy. The Contractor must continue to treat cardholder data as confidential upon contract termination.

8.6. The Contractor must provide the State's Contract Administrator with an annual Report on Compliance (ROC) or an Attestation of Compliance (AOC) if a ROC has not been completed, showing the contractor is in compliance with the PCI Data Security Standard. The Contractor must notify the State's Contract Administrator of all failures to comply with the PCI Data Security Standard.

9. Protection of the State's Confidential Information. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will:

the **Hosting Provider** for SOM Software and Data must be FedRAMP authorized, and Contractor must maintain hosting in a FedRAMP authorized computing environment for the Hosted Services throughout the Term, and in the event the contractor is unable to maintain FedRAMP authorization, the State may move the Software and data to an alternative hosting provider, at contractor's sole cost and expense;

Contractor must maintain a FedRAMP authorization or an annual SSAE 18 SOC 2 Type 2 audit based on NIST moderate controls for the Hosted Services throughout the Term;

ensure that the Software is securely hosted, supported, administered, and accessed in a data center that resides in the continental United States, and minimally meets Uptime Institute Tier 3 standards (www.uptimeinstitute.com), or its equivalent;

maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State's Confidential Information that comply with the requirements of the State's data security policies as set forth in the Contract**,** and must, at a minimum, remain compliant with FISMA and the NIST Special Publication 800-53 (most recent version) MOD Controls using minimum control values as established in the applicable SOM PSP's, and must, at a minimum, remain compliant with FISMA and the NIST Special Publication 800-53 (most recent version) HIGH Controls using minimum control values as established in the applicable SOM PSP's;

provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of the State's Confidential Information and the nature of such Confidential Information, consistent with best industry practice and standards;

take all reasonable measures to:

secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services against "hackers" and others who may seek, without authorization, to disrupt, damage, modify, access or otherwise use Contractor Systems or the information found therein; and

prevent (i) the State and its Authorized Users from having access to the data of other customers or such other customer's users of the Services; (ii) the State's Confidential Information from being commingled with or contaminated by the data of other customers or their users of the Services; and (iii) unauthorized access to any of the State's Confidential Information;

ensure that State Data is encrypted in transit and at rest using AES encryption and a key size of 128 bits or higher 256 bits;;

ensure that State Data is encrypted in transit and at rest using currently FISMA / FIPS PUB 140-2 validated encryption modules

ensure the Hosted Services support Identity Federation/Single Sign-on (SSO) capabilities using Security Assertion Markup Language (SAML) or comparable mechanisms;

ensure the Hosted Services implements FIPS/NIST compliant multi-factor authentication for privileged/administrative and other identified access; and

assist the State, at no additional cost, with development and completion of a system security plan using the State's automated governance, risk and compliance (GRC) platform.

SCHEDULE H

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES

SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.1 Definitions

1.2 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.3 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.1 Responsibilities of the Contracting Government Agency.

2.2 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.1 Responsibilities of the Contractor.

3.2 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is

executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.1 Security Violations.

4.2 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.3 Security violations can justify termination of the appended agreement.

4.4 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.1 Audit

5.2 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.1 Scope and Authority

6.2 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.3 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.4 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.5 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.6 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES

SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

Exhibit A – Table 1 – Business Specification Worksheet

A	B
Business Specification Number	**Business Specification**
MANDATORY MINIMUM	The system must have a modifiable Commercial off the Shelf (COTS) Sex Offender Registry application supporting an offender population of 2,500 or more; that has been implemented and supported by the primary Vendor for a minimum of 3 years.
	While the solution may be integrated on a global platform used by other entities, the Vendor must commit to the needs and enhancements required by the State of Michigan (SOM) and to confirm such needs will not be delayed or denied due to other entities using the same platform.
REQUIRED	**TECHNICAL SPECIFICATION**
1.0	System must be a highly configurable/highly adaptive program based on the current and future needs of the SOM. Ability to meet changes initiated by Michigan legislation, or judicial body within the timeframe established by those entities. Ability to meet changes initiated by Michigan State Police (MSP) policy changes, etc.; and within six months or less. System must comply with current SOR Act http://legislature.mi.gov/doc.aspx?mcl-Act-295-of-1994, and any future versions of the SOR Act
2.0	The System must have multiple user levels with specific functions/capabilities: Read only: Have access to view only offender data, cannot make any modifications/entries. No LEIN or NCIC access or visibility. (prosecutor office's, Indian Tribes, college/university police, Hospital Police/Security.) Read/write: Have access to manipulate data within certain fields except for those locked by Super Admin. (local and state law enforcement) Admins: Have access to manipulate data within fields, except for those locked by Super Admin. (Select SOR Unit Staff and SOR Enforcement)

	Super Admins: Can designate user levels, lock any field in the system, lock offender records, publish offender records to Public Website, hide any data fields or data sets/tabs, and have overall access to the system other than access that may be deemed programing and/or coding. (Lead SOR Enforcement Officer, SOR Manager, and SOR Coordinator)
3.0	System should have a “simple search,”” free search,” and” detailed search” functionality. Simple search – allows a user to search the System by one or more of the following: • Offender Name • DOB • Michigan SID • Michigan Offender Registration Number • Michigan Department of Corrections Number • DLN/ID Detailed Search – provides the ability to search on a broader perspective. Would include fields from all sections and is to include date range. Free search – provides a one field search by key word or words.
4.0	System must allow a user to create and save commonly used searches.
5.0	System must have a color-coding system that identifies risk/classifications, juveniles, non-published records, offender status, parole/probation, etc.
6.0	System must present in consistent text (such as all caps) and spacing throughout all data fields.
7.0	System must have logic for consistency in abbreviations. Example: St. Clair versus Saint Clair; and Ste. versus Suite, etc.
8.0	System must have spell-check logic.
9.0	System must have a primary offender data set such as, but not limited to: • Full Name • DOB • Photo • MI Registration # • Current address(s) and type. • Status • Tier/Risk/Classification • Compliance • Registration Duration

	• Parole Status • Juvenile (Yes/No) • Published
10.0	System must be able to recognize mandatory data fields based on "triggers." i.e. If offender reports a vehicle then VIN, MKE, model, color, and year is required.
11.0	System is to accept a data transfer and house MSP records previously stored in our HP Records Manager System.
12.0	System must have a Wizard based feature for add new offender.
REQUIRED	**REGISTRATION/VERIFICATION**
13.0	When applicable, the System must note if the offender has a guardian or custodian within the offender's primary data set.
14.0	If an offender is marked as non-published System should display reason/wording as to why the record is non-published as part of the primary data set of the offender such as, but not limited to: • Offender is an adjudicated juvenile. • Offender is non-Michigan resident. • Offender's convicted offense doesn't require registration. • Offender was granted removal from registry by court order.
15.0	System must provide a "pop-up" for users when modifying a juvenile record in any manner, that indicates the offender is a juvenile and the user must somehow acknowledge or agree to the protection of juvenile information prior to moving forward.
16.0	System must capture digital signatures (wirelessly) with current product, Topaz T-L(BK)462 Model Series SignatureGem LCD 1x%. Additionally, be compatible with other potential signature products. https://www.topazsystems.com/siggemlcd1x5.html
17.0	System must operate in conjunction with ID swipers or other identified apparatuses with established parameters for scanning state ID's and drivers licenses.
18.0	System shall accommodate Address Types "dropdown list" such as, but not limited to: • **Home** • **Secondary –** Girlfriends, a second home (aka cabin) • **Temporary -** vacationing • **Mailing –** PO Box, or wanting their mail to go to a relative's home, etc. • **Incarcerated** – options should be given for Incarceration Type (County Jail, Prison, etc.) with facility name (Muskegon Correctional Facility, Bellamy Creek Corrections, etc.) System should be able to automatically calculate time if initiated.

	• **Rehab/Hospital/Nursing Home** (name of facility and address.) • **Homeless** (enter city, state, zip and county.) • **Deported** (enter the country.) • **Absconder** (enter last known city, state and zip.) System must require a minimum of one address: home, incarcerated, absconder, homeless, rehab/hospital/nursing home or deported. For all new entries of a new home or incarceration type the System shall automatically populate an end date to the last previous home or incarceration address. For all other address types, the system should ask the user if they would like to add an end date and highlight the possible address types in question. Historical/current address data and incarceration addresses must be presented together on a single tab; placed in chronological order with most recent displayed first. To present for historical view and management. Incarceration entries must be shaded a different color to stand out.
19.0	For Homeless type, System shall prompt user to ask offender and enter details for a frequent sleeping spot such as major cross street or landmark (captured in a “notes”.)
20.0	System must assign offenders to a responsible county jurisdiction based on home address for providing notifications, running reports, conducting searches, of offender’s they would be responsible for. Within each county the system must be able to display a breakdown of offenders by group, city, and/or township; based on address.
21.0	The System shall accommodate offender statuses such as, but not limited to: • **Active** • **Inactive** • **Incarcerated** • **Pending Out of State** – Offender updates their address out of state. (Once made to this status, can only be changed by Admin and Super Admin to another status.) • **Out of State** – Confirmed Offender is out of state. (Accessible to Admin/Super Admin only.) • **In Review –** Is under review by an Admin or Super Admin. (Once made to this status, can only be changed by Admin and Super Admin to another status.) • **Canceled –** Registration no longer exists. Remains for historical purposes and is locked. (Accessible to Admin/Super Admin only.) • **Pending Registration –** Offender is said to be moving/coming to MI, waiting to confirm. • **To be Reviewed** – Is a new registration. (Once made to this status, can only be changed by Admin and Super Admin to another status.) • **Deceased** (accessible to Admin/Super Admin only.)

22.0	When an offender's address is updated in the system as incarcerated, the System should change offender status to "Incarcerated." If offender's address is updated to a Michigan home or temporary address when the last address was incarcerated, the offender's status should automatically be made "Active." When an offender's status is made "Canceled" or "Deceased" the system must automatically remove the offender profile from the public website.
23.0	System must make the status of any newly created registration as (new to Michigan, entered by Michigan Department Corrections, Federal Prison releases, etc.) "To be Reviewed." These offenders will remain unpublished at the public facing website until a member of the SOR Unit has confirmed record is complete.
24.0	If an offender updates their address to an out of state address the system should automatically update their status to "Pending Out of State."
25.0	The "In Review" status can only be used by an Admin or Super Admin. System must automatically capture and present a user email of whom is reviewing the record on the primary tab. A list of Admins and Super Admins will be provided to vendor by MSP.
26.0	The System must list offenses chronologically, by conviction date, with the most recent date first.
27.0	System should provide the ability for Michigan driver's license or personal identification scanning to pull up an offender's record for editing/updating.
28.0	System must require mandatory data fields be entered prior to allowing record to be saved. Fields to be identified by SOR Unit.
29.0	System must be able to: • "auto-tier" offenders • Determine verification frequency • Determine publishing • Determine registration duration • Set conviction type (juvenile/adult) If victim age is unobtainable Admin user must have the capability to manually tier offense/offender. System must automatically set anniversary dates based on offender's birth month and Tier/risk/classification schedule.
30.0	When an offender misses a verification cycle, the System should automatically flag as "non-compliant" and identify that they RSO has "Failed to Verify" in verification history.

31.0	If an offender is incarcerated or out of state during a verification period, the System must auto-populate the verification history with the status of Incarcerated or Out of State so as to not present holes/blanks in the verification history.
32.0	The System must provide warnings, and highlight data fields in question, if entries made may cause erroneous information in the record and/or in cases of omitted information such as, but not limited to: • New entry warns if there is an existing record for the same offender • If a required field is omitted • Character length errors (SID, DOB, DLN, SSN, etc.) • Use of future dates
33.0	System must accommodate noncompliant reason such as, but not limited to: • Failed to register • Address violation • Employment violation • Campus violation • Fee violation • Form violation • ID violation • Email/internet violation • Vehicle violation • Failed to verify • School safety zone violation • Palm Print • Telephone • Immigrant Documents • Professional License • False Information
34.0	The system shall automate violations such as, but not limited to: • **Fee violation** (missed fees) • **Palm Prints** (when = No) • **ID** (None or expired) • **Failed to Verify** • **Address** (If an Address Type of “Absconder” is selected, an Address violation should automatically be added.)
35.0	System must story a history of offender’s violations (Fee, Palm Print, ID, Failed to Verify, Address, etc.)
OPTIONAL	**REGISTRATION/VERIFICATION**

36.0	System is to have Michigan street/address logic to prepopulate city, state, county, country, and zip when recognizing an address.
37.0	When entering work, school, or volunteer business name, the System shall be able to store data set to recognize/recall for future reference. (Example: Qdoba, entered for offender A; later offender B worksite is the same – System recalls business name and prepopulates. Whether by presenting a predetermined list or begins to prepopulating the predetermined address)
38.0	System must notify the Admins and Super Admins when there is a "To Be Reviewed" record. Notifications may be via email to an Admin user, assigned mailbox, or pop-up notification upon entry.
REQUIRED	**INVESTIGATIVE/MONITORING**
39.0	System must accommodate the following data fields for tips such as, but not limited to: • Date of tip submission (must be auto-stamped) • Type – How we received the tip • Tip • Status • Result • Notes • Absconder Notes
40.0	System must collect notes accumulatively, and present notes saved chronologically with most recent first. Users may enter notes and must be requested to save prior to the system accepting submission. Once offender data record is saved and closed the user will not be able to edit their notes. User must receive a warning that no changes can be made after record is saved/closed. The system must automatically date-stamp with the date of entry, capture the user email that entered, and present along with the user notes in the notes section. System must be able to accept multiple note entries and produce in an at-a-glance historical view.
41.0	System must accommodate the following tip statuses: • New • Closed • Under Investigation • Warrant Issued • Warrant Requested
42.0	System must capture tip types submitted by the public such as, but not limited to: • Public – Law enforcement contact • Public – SOR Hotline

	• Public – MI SOR Public Website Allowing us to track how the public best communicates to/with MSP SOR. System must capture and prepopulate tips submitted to the public website to the SOR registry.
43.0	System must accommodate the tip result such as, but not limited to: • Arrested – SOR Violation • Arrested – Other Violation • Arrested – SOR & Other Violation • No prosecution • Found compliant • Unfounded • Warrant Denied • Other, See notes
44.0	System must automatically assign entered Tips to the responsible county jurisdictions; sending notification to the law enforcement agency (County, PD, DPS, etc.) that has jurisdiction over related offender. Jurisdiction is based on offender's home address.
45.0	For Tips marked as new, the System is to provide a pop-up warning upon opening of an offender's record that a new tip has been entered.
46.0	When entering a tip, the System must automatically be marked as "new" tip status, unless another type is selected.
47.0	System must have data set fields for Absconders such as, but not limited to: • Date Absconded (based on selection of address violation reason) • User email that entered violation (system must auto-stamp user email that made address violation entry) • Date located • Where located • Address Lead • Date of Address Lead • Address Lead sources • Address Lead Unfounded (checkbox) • Last checked date • Next follow-up date • Private • Tracking Notes • Tracking Analyst (system must auto-stamp user email making entry) • Tracking date (system must auto-stamp date if anything entered and saved in Tracking notes. • Tracking user email

	System must be able to accept multiple entries of Leads and Tracking information and produce in an at-a-glance historical view.
48.0	System must have a list box for Lead Sources with source types such as, but not limited to: • DHS • SOS • TLO • NSPOW • NLETS • NCMEC • TIPSTER • RETURN ENVELOPE • OTHER (with free text)
49.0	System must accommodate notes area for **absconder** research, collect notes accumulatively, and present notes saved chronologically with most recent first. Users may enter notes and must be requested to save prior to the system accepting submission. User must receive a warning that no changes can be made after notes are saved. Once "save" is selected the system must automatically date-stamp with the date of entry, capture the user email that entered, and present along with the user notes in the Absconder notes section.
50.0	System must provide a mapping function to identify school zones (GIS).
51.0	System should distinguish those offenders who live within a school's safety zone but are exempt. When an offender is updating his/her address at law enforcement agency, System should provide warning when address is within school safety zone, unless offender is exempt.
52.0	System must provide a "sweep" wizard for offender mapping. Mapping is to include best/ direct/clear routes during enforcement sweeps. based on a starting point and end point. System must have the ability to create a mapping list of offenders and save. System must distinguish those offenders who live within a school's safety zone but are exempt.
53.0	System must provide the ability for each jurisdiction to create and save its own offenders map searches, and ability to draw and save unique boundaries.
54.0	System must automatically map a homeless offender to the center of the city entered or "sleeping spot" if identified by registrant.
55.0	As part of the "sweep" wizard, system must have a mobile platform with the ability to adapt to multiple electronic devices (I-pad, I-phone, android, tablet, etc.)

56.0	When using the sweep wizard the System must provide photos for each offender on their address when viewing a map. When clicking on the photo the system will provide three (3) options, “resident check completed, ““quick view,” or “full view.” **Resident check completed** – provides the date the offender last had a successful resident check. **Full view** – provides offender’s complete record for edits/updates. **Quick view** – includes, but not limited to: • Name • DOB and physical attributes. • Current address(s) and type. • Current phone number(s). System must provide a “sweep” wizard for offender mapping. Mapping is to include best/ direct/clear routes during enforcement sweeps; based on a starting point and end point.
REQUIRED	**SAVED FORMS**
57.0	System must have the ability to accept documents for upload and house an unlimited number of documents within offender’s data record.
58.0	System must have the ability to maintain and prepopulate fields applicable within printable forms loaded (as identified by MSP).
59.0	System must have the ability to add registration/verification forms and recall the coinciding form automatically when a specific risk/classification is selected such as, but not limited to: • MI Residence Check/Invest Reports • Michigan Certified Rec • Registration Form • Verification/Update Form
60.0	System must have the ability to automatically save to offender records any digitally signed forms.
REQUIRED	**GENERAL**
61.0	System must send required data to NCIC as outlined by NCIC standards. The System must have the ability to send additional data that is not required but is collected by MSP and accepted by NCIC. Future changes, in data sent, may be required in order to maintain compliance with NCIC. Any changes made to ensure NCIC compliance should be considered maintenance.

	When an offender's status is made "Canceled" or "Deceased" the system must automatically remove the offender profile from the NCIC.
62.0	All offenses should require victim age or an allowable substitute. If offense was not committed against a specific person or victim age cannot be obtained, then user should have the option to select "Nonspecific person/victim." Example: Computer crimes that are not perpetrated against a specific individual.
63.0	System must support web services currently provided to entities such as Michigan Department of Health and Human Services, and Michigan Department of Licensing and Regulatory Affairs.
REQUIRED	**PUBLIC-FACING WEBSITE**
64.0	System must provide a public-facing website that feeds data to registry system and is fed data by registry System. i.e. Website will accept investigative tips and feed into the registry System to corresponding jurisdiction for where the offender lives; to be addressed by law enforcement.
65.0	System must allow public users to view and interact through use of their phones or other electronic devices (I-pad, I-phone, android, tablet, etc.)
66.0	Website must display what is currently shown and will include but not be limited to: • Offender Compliance Status • Offender physical description • Photo (If no SOS, system is to display MDOC or arrest photo) • Address • Employment • School Attendance • Tier (if applicable) • Offense • Incarceration • Offender MI Dept. of Correction ID number • Offender exemption status, to live in school safety zones.
67.0	System must have the capability for users to upload photos or documents to send with their tips.
68.0	Website will map offender addresses for the public and return results of offenders in the user's vicinity, up to 15 miles. Options to be completed by a user address or GPS location. System must provide photos for each offender on their address when viewing a map in the system.

69.0	System shall allow public users to sign-up and receive emails or text messages regarding when an offender moves to, attends school near or works in the user's vicinity.
OPTIONAL	**PUBLIC-FACING WEBSITE (Additional Items)**
70.0	System shall allow offenders to sign-up and receive email notifications regarding verification reminders or other pertinent information through the public facing website. Must include the ability to unsubscribe at any time.
REQUIRED	**MOBILE APPLICATION**
71.0	Must build an API to the MSP Mobile application (iOS and Android). Mobile application provides data reflected on the public website and allows for offender searches by name, address and location. Additionally, allows users to submit anonymous tips.
72.0	The Contractor's solution must include a RESTful Web Service that returns all data in JSON format.
73.0	There must be two search functions (search by name and search by location) will need to accept the search data provided by the user and return results based on that data.
74.0	For the search by location, our preference is that the Contractor use Google Places to geocode the coordinates that are returned to our application.
75.0	Exhibit 1, Attachment 2 provides the data that will need to be returned to the system so that it can be displayed by the MSP Mobile Application.
REQUIRED	**ONLINE UPDATES**
76.0	System must have a secure online tool for current offenders to Pre - update their personal registration information.
77.0	System must allow offenders to complete update(s) through their phones or other electronic devices (I-pad, I-phone, android, tablet, etc.)
78.0	The online tool must have the ability to pull an offender's registry information (associated with the verification requirements) for updating; based on System authentication. Including, but not limited to: • Date of birth • Last 4 of their SSN • SOR Registration #
79.0	Once authenticated, offenders must have select record details presented and must confirm if the profile is them or not; prior to being provided access to their personal information. If no, the session is canceled.

80.0	System must provide a disclaimer in a manner that identifies *rules and conditions* of Pre-updating and must require an acknowledgment from user prior to providing access to their personal information. Rules and conditions to be provided by MSP.
81.0	System online tool must only show the offender's current information. Nothing previously removed nor any historical data. Offender information must be displayed in group setting similar to SOR registry system and have the ability to skip to desired sections. The online tool must have the ability to "go back" to a desired data set without having to restart entry process.
82.0	If offender responds "Yes" to changing an address or phone the System should prompt with "Do you have another address (phone) to update? No/ Yes."
83.0	System online tool will allow for entry of every type. i.e. There are multiple different phone types that the offender must be allowed to enter all through one updating session, including but not limited to: • Home (only 1 allowed) • Secondary • Temporary • Mailing
84.0	Offender must have the ability to deactivate information. However, information removed must remain in the SOR registry history data for investigative purposes. If offender removes an entry within the online system, the System must enter the date of deletion as the "end" date in the SOR Registry system. (phones, addresses, etc.) i.e. If offender no longer has a home phone and removes it from the online session, the system should use the date the offender removed the number through the online tool as the "End Date" on the corresponding phone number in the SOR Registry system.
85.0	System must be able to provide warnings if data seems to be inaccurate or incomplete.
86.0	All changes made by an offender during a session utilizing the online tool will be placed in a "pending" status until offender verifies the changes in person at a local law enforcement agency.
87.0	Updates made within the online tool will inform offenders that submitted changes/updates will be available for 5 days and that the individual must present in person to a local law enforcement (LE) agency to complete the updating process.
88.0	System must make "pending" changes accessible to any law enforcement agency so they may be verified and accepted. Data will be accepted or rejected by checking line by line item, no grouping. Upon acceptance, offender data record will open with all populated applicable fields for additional review. While data may be accepted, data will not truly be saved to the data record until the record is "saved" in the registry system by LE.

	Once agency saves changes they are considered finalized; both the System and online public facing website are updated.
89.0	System will allow only admins to delete any unaccepted “Pending” items from the system.
90.0	System must have a final review page prior to submission.
91.0	System must have the ability to provide user with the option of having their session details emailed to them. If this feature is utilized the System must ask user to if email provided is a personal email. If yes and applicable to the offender as a required field, system must add it to the “Internet” tab in the SOR Registry system.
REQUIRED	**REPORTING**
92.0	System must be able to provide real-time ad hoc reporting capability. System must have the ability to build, run, and save reports based on any data field within the System. (Such as who hasn't had a residence check, who has, etc.)
93.0	System must have the ability to run a report of actions completed in the System in a date range and assisting other fields. (See System search Technical Specification 3.0)
94.0	System must provide a method for jails to print a list of all the offenders currently in their jail; with an option to users to receive weekly notifications containing a list of offenders in their jails.
95.0	For administrative use only: System must be able to upload letter templates provided by MSP admins, prepopulate applicable offender data, and generate letters for printing and saving. (System should have no limits to letter templets uploaded and saved.) System must be able to generate letters from a Template within the system.
96.0	System must provide options to export to: excel, word, Adobe PDF, etc.
OPTIONAL	**REPORTING**
97.0	System must have the ability to create reporting schedules for saved searches that will automatically run and produce the search results. i.e. User may want a report for all offender failing to verify, with specific data, run the first of every month, the System would have the capability for users to create, save, and schedule the system to run this as an ongoing cycle.
98.0	System to provide the ability to receive weekly notifications of a list of offenders in their jails.

REQUIRED	AUDIT
99.0	System must have the ability to audit changes/modifications on every data element within the System.
100.0	System must require at least one identifier to conduct an audit search. Identifier options should include but not be limited to: • By Agency/ORI • By User • By Offender (Registration #, or name) • Start or End Dates • And, in a date range
101.0	System must have the ability to provide the following data within an audit inquiry, including but not limited to: • Provide what changes were made showing before/after. • Provide the name of user, email address, their associated agency and ORI that made the change. • Audit report results must appear in chronological order, with the most recent action first. • Provide date and time of change. • Provide type of action (New action/Modification/Deletion)" • Must be able to export report to Excel
REQUIRED	**FEE**
102.0	System shall auto-stamp date, time, agency name, and user name in fee payment section.
103.0	System must provide at a minimum: • Date of transaction • Time • Status (collected, indigent, incarcerated and out-of-state) • Agency Name • User Name • Amount (auto-populate with increments of $50, not to exceed $550.) • Payment Type (cash, check, money order, or credit card) (if status is incarcerated or out-of-state auto populate with “other”) o Check/Money Order #, triggered if check or money order is selected as Payment Type. • Receipt ID • Notes • Capture agency that collected a fee. • Capture & identify when more than one fee is collected at a time. • Initial/Annual Fee (dropdown with option of “Initial” or “Annual”.)

104.0	If fee status is indigent for 90 days, on the 91st day, 12:00 a.m. EST, System must automatically make offender non-compliant for fees.
105.0	System must be able to alert user if the maximum of $550 has been collected from a registrant.
106.0	System must maintain a detailed billing summary for each offender registered.
107.0	System must provide the ability to run fee reports in order to audit and reconcile billing with invoices that are created by the MiCARS application.
108.0	System must be capable of making changes in short period; for fee processes and/or amounts if changes are implemented by Michigan State Police or by legislation.
REQUIRED	**ONLINE PUBLIC FEE PAYMENT SYSTEM**
109.0	System shall have a secure public facing fee payment system.
110.0	System must allow users to complete SOR fee payments through their phone; with the ability to adapts to multiple electronic devices (I-pad, I-phone, android, tablet, etc.)
111.0	The payment screen must include, but not be limited to the following fields: • Offender name • SOR registration number • Date of transaction • Time • Amount (increments of $50, not to exceed $550) • Payment Type (credit/debit card) • Receipt ID Additionally, public facing fee payment screen must allow for multiple $50 payments reflecting line by line item but allow the user to pay together.
112.0	Public facing screen must integrate with System to update and prepopulate the SOR Registry system fee section.

Exhibit C - Pricing

Pricing: Sex Offender Registry (SOR) Solution		
Contract Period	**Contract Year**	**Cost**
Base Period (one 5-year period)	Base Year 1[A]	$380,000
	Base Year 2[B]	$380,000
	Base Year 3[B]	$380,000
	Base Year 4[B]	$380,000
	Base Year 5[B]	$380,000
Subtotal for Base Period (5 years)		**$1,900,000**
Option Period (two 1-year options)	Option Year 1[B]	$380,000
	Option Year 2[B]	$380,000
Grand Total for the Entire Contract Period (7 years)		**$2,660,000**

[A] Includes the Coplogic implementation services and post-production warranty support shown in the next table.

[B] Includes ongoing maintenance, support, and training by Coplogic as well as estimated third-party cloud service provider hosting fees.

Milestone-Based Payments for System Implementation		
#	Milestone	Payment Amount
1	**Kickoff Meeting & Design Phase**	*(payment at go-live)*
2	**Delivery of the Web-based Registry Application**	*(payment at go-live)*
3	**Delivery of the SOR Processing Application**	*(payment at go-live)*
4	**Delivery of the General Public SOR Web Application**	*(payment at go-live)*
5	**Delivery of the Required Interfaces, as available***	*(payment at go-live)*
6	*Please note that additional fees apply to these optional interfaces (specifically: the Federal Bureau of Prison, Michigan Department of Health and Human Services – BRIDGES (food card), SMRS, and ICE)*	*TBD*
7	**Conversion**	*(payment at go-live)*
8	**UAT, Training Documentation and Train-the-Trainer**	*(payment at go-live)*
9	**Go-Live, Implementation and Warranty Support**	$380,000
	Total for System Implementation	**$380,000**

*Coplogic is committed to delivering the required interfaces, as available. Please note that the go-live milestone completion and payment is **not** dependent upon the development and activation of all required interfaces. Interfaces with external third-parties involve many aspects that are outside of our control and impact the timeline. Coplogic expects that MSP will facilitate meetings and cooperation from third-party interface owners.

Coplogic Rate Card for Ancillary Professional Services	
Resource Type	**Hourly Rate**
Project Manager	$175
Business Systems Analyst/Systems Analyst	$135
Senior Developer	$150
Developer	$150
Network Engineer	$110
Trainer	$90
Implementation Specialist	$90

- Training includes up to five (5) onsite sessions. There is not any limit on web-based/remote training, both during implementation and on an ongoing basis beyond the initial implementation).